Office of Technology Assessment
Congressional Board of the 102d Congress

GEORGE E. BROWN, JR., *California, Chairman*

TED STEVENS, *Alaska, Vice Chairman*

Senate	House
EDWARD M. KENNEDY *Massachusetts*	JOHN D. DINGELL *Michigan*
ERNEST F. HOLLINGS *South Carolina*	CLARENCE E. MILLER *Ohio*
CLAIBORNE PELL *Rhode Island*	DON SUNDQUIST *Tennessee*
ORRIN G. HATCH *Utah*	AMO HOUGHTON *New York*
CHARLES E. GRASSLEY *Iowa*	*(Vacancy)*

JOHN H. GIBBONS
(Nonvoting)

Advisory Council

CHASE N. PETERSON, *Chairman*
University of Utah
Salt Lake City, Utah

JOSHUA LEDERBERG, *Vice Chairman*
Professor
Rockefeller University
New York, New York

CHARLES A. BOWSHER
Comptroller General of
the United States
Washington, D.C.

LEWIS M. BRANSCOMB
Director of Science, Technology &
Public Policy Program
Albert Pratt Public Service Professor
Harvard JFK School of Government
Cambridge, Massachusetts

MICHEL T. HALBOUTY
Chairman of the Board &
Chief Executive Officer
Michel T. Halbouty Energy Co.
Houston, Texas

NEIL E. HARL
Professor
Department of Economics
Iowa State University
Ames, Iowa

JAMES C. HUNT
Chancellor
Health Sciences Center
University of Tennessee
Memphis, Tennessee

HENRY KOFFLER
President Emeritus
University of Arizona
Tucson, Arizona

MAX LENNON
President
Clemson University
Clemson, South Carolina

JOSEPH E. ROSS
Director
Congressional Research Service
The Library of Congress
Washington, D.C.

JOHN F.M. SIMS
Vice President, Marketing
Usibelli Coal Mine, Inc.
Fairbanks, Alaska

MARINA v.N. WHITMAN
Vice President & Group Executive
Public Affairs Staffs Group
General Motors Corporation
Detroit, Michigan

Director
JOHN H. GIBBONS

The views expressed in this background paper are not necessarily those of the Board, OTA Advisory Council, or individual members thereof.

THE FBI FINGERPRINT IDENTIFICATION AUTOMATION PROGRAM: ISSUES AND OPTIONS

Background Paper

CONGRESS OF THE UNITED STATES
OFFICE OF TECHNOLOGY ASSESSMENT

J952-96

For sale by the U.S. Government Printing Office
Superintendent of Documents, Mail Stop: SSOP, Washington, DC 20402-9328
ISBN 0-16-035974-0

Recommended Citation:

U.S. Congress, Office of Technology Assessment, *The FBI Fingerprint Identification Automation Program: Issues and Options—Background Paper*, OTA-BP-TCT-84 (Washington, DC: U.S. Government Printing Office, November 1991).

Foreword

The criminal justice process depends on quick and accurate identification of persons arrested for violations of the law. Police, prosecutors, and judges need to know the extent of any arrestee's prior criminal record when making detention, bail, charging, and sentencing decisions.

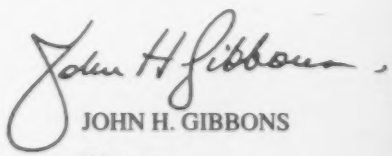
Fingerprint identification is the most widely accepted method for establishing positive identification, and for linking an arrestee with any prior criminal record. Fingerprinting helps assure public safety by identifying repeat offenders who may need to be detained while a case is pending. It also helps protect the constitutional rights of all persons who undergo criminal record checks—whether arrestees or job, license, and security clearance applicants—by minimizing the chances of misidentification.

The Federal Bureau of Investigation (FBI) has historically played a key role in providing fingerprint identification and criminal history records on a nationwide basis. But the FBI's fingerprint system is technically obsolete and incompatible with the many more advanced State and local systems. The FBI's criminal history file is still not fully automated and complete—as many as half of the arrests listed are missing information on the final disposition of the case.

OTA's background paper assesses the FBI's strategic plans to modernize and fully automate its fingerprint identification and criminal history record system. The paper focuses on key assumptions that will affect the sizing and procurement of the new FBI system, and on other related steps that appear necessary to ensure complete and up-to-date record systems. These include full implementation of a Federal/State/local partnership for maintaining and exchanging fingerprint and criminal history records; enactment of an interstate compact or Federal legislation setting out uniform rules for the exchange of such records; standards and funding for improving criminal history record completeness and disposition reporting; and privacy and security protections for electronic fingerprint and record information.

This study was requested by Rep. Don Edwards, Chairman, Subcommittee on Civil and Constitutional Rights, House Committee on the Judiciary.

OTA benefited from discussion at a July 1991 workshop, comments on earlier drafts by many law enforcement and criminal justice experts, and prior reports on this topic prepared by or for criminal justice agencies. OTA appreciates the assistance of the FBI and Bureau of Justice Statistics; Federal, State, and local agencies that use FBI records; the FBI's National Crime Information Center Advisory Policy Board; SEARCH Group, Inc., a State/local consortium on criminal justice; and groups concerned with the civil liberties implications of criminal justice record systems. The content of the background paper is, however, solely the responsibility of OTA.



JOHN H. GIBBONS
Director

The FBI Fingerprint Identification Automation Program
Workshop Participants
July 29, 1991

Kenneth Bentfield
Office of Information Systems Management
Minnesota Department of Public Safety

Joseph P. Bonino
Records and Identification Division
Los Angeles Police Department

Bruce Brotman
Identification Division
Federal Bureau of Investigation

Gary Bush
Information Services Branch
Kentucky State Police

Gary R. Cooper
SEARCH Group, Inc.

Dennis DeBacco
Criminal Information Services
Nevada Highway Patrol

Lamont Edwards
Criminal Justice Information System
Maryland Department of Public Safety

Gary D. McAlvey
Bureau of Identification
Illinois State Police

Maurice A. Ross
U.S. Department of Justice

Marc Rotenberg
Washington Office
Computer Professionals for Social Responsibility

Bernie Shipley
Criminal History Record Improvement Program
Bureau of Justice Statistics

Roland Sutfin
Information Systems Engineering

George Trubow
Center for Informatics Law
The John Marshall School of Law

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the workshop participants. The workshop participants do not, however, necessarily approve, disapprove, or endorse this report. OTA assumes full responsibility for the report and the accuracy of its contents.

The FBI Fingerprint Identification Automation Program: OTA Project Staff

John Andelin, *Assistant Director, OTA*
Science, Information, and Natural Resources Division

James W. Curlin, *Program Manager*
Telecommunication and Computing Technologies Program

Project Staff

Fred B. Wood, *Project Director*

Administrative Staff

Liz Emanuel, *Office Administrator*

Jo Anne Young, *Secretary*

Karolyn St. Clair, *PC Specialist*

Reviewers and Contributors

James R. Amos
Bureau of Records and Information Services
Pennsylvania State Police

Kier T. Boyd
Technical Services Division
Federal Bureau of Identification

Robert J. Bradley
Division of Information Systems
Missouri State Highway Patrol

William C. Corley
State Bureau of Investigation
North Carolina Department of Justice

D.B. Cramer
Records and Identification Division
Pennsylvania State Police

Charles Cunningham
Identification Systems Section
Immigration and Naturalization Service

Jim Dempsey
Subcommittee on Civil and Constitutional Rights
House Committee on the Judiciary

Patrick J. Doyle
Division of Criminal Justice Information Systems
Florida Department of Law Enforcement

Gene Draper
Texas Criminal Justice Policy Council

Thomas E. Ewald
Defense Investigative Service

Pete Falcone
Civil Aviation Security Office
Federal Aviation Administration

Don Flynn
Identification Division
Federal Bureau of Investigation

Philip W. Gasiewicz
Federal Investigations Processing Center
Office of Personnel Management

Janlori Goldman
Privacy and Technology Project
American Civil Liberties Union

Jim Gildea
Enforcement Division
Immigration and Naturalization Service

Earl Gillespie
Criminal Justice Information Systems
Maryland Department of Public Safety

Owen Greenspan
New York State Division of Criminal Justice Services

Fred Hagan
Alameda County (California) Sheriff's Office

John Hanby
PRC Inc.

Karen Hess
U.S. Border Patrol

Gwen A. Holden
National Criminal Justice Association

Jim Holst
Interpol

Walter Johanningsmier
Identification Division
Federal Bureau of Investigation

Mildred Jones
National Agency Check Division
Defense Investigative Service

Nolan E. Jones
Justice and Public Safety Committee
National Governors Association

Robert A. Jordan
Identification Division
Federal Bureau of Investigation

Bill Kardash
Identification Division
Federal Bureau of Investigation

William G. Keller
Western Identification Network, Inc.

Stanley Klein
Identification Division
Federal Bureau of Investigation

Gil Kleinknecht
Enforcement Division
Immigration and Naturalization Service

Arthur Law
IBM Corp.

Valcocean Littles
Records and Identification Section
New Jersey State Police

Charles Mandigo
Federal Bureau of Investigation

Anita Mauck
San Diego County (California) Sheriff's Office

Ed McGuire
Management Control and Security Services
Bureau of the Census

David Nemecek
Technical Services Division
Federal Bureau of Investigation

Jim Olech
U.S. Border Patrol

Julie Peternick
PRC Inc.

Dallas G. Piper
Central Records Division
Michigan State Police

James Pulio
Immigration and Naturalization Service

Emmet Rathbun
Identification Division
Federal Bureau of Investigation

Art Rehkemper
Forensic Services
U.S. Secret Service

Richard Reneau
Santa Clara County (California) Sheriff's Office

Dean Renfrow
Criminal Investigation Division
Oregon State Police

Tom Roberts
Identification Division
Federal Bureau of Investigation

James Sprung
MITRE Corp.

Douglas Smith
California Department of Justice

Phil Slowinski
Interpol

John Sullivan
Identification Division
Federal Bureau of Investigation

Arthur Thomas
Identification Division
Federal Bureau of Investigation

Enrico Togneri
Washoe County (Nevada) Sheriff's Office

James D. Vaden
NEC Technologies, Inc.

R. Lewis Vass
Virginia State Police

Fred Wynbrandt
Identification and Information Branch
California Department of Justice

Virgil Young
Identification Division
Federal Bureau of Investigation

Joe Zahuronis
Inspection Service
U.S. Postal Service

NOTE: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the reviewers. The reviewers do not, however, necessarily approve, disapprove, or endorse this report. OTA assumes full responsibility for the report and the accuracy of its contents.

Contents

Page

Summary 1

The Context for Ident Automation 5
- The National Fingerprint File/Interstate Identification Index (NFF/III) Concept 7
- Interstate Compact or Federal Legislation on Criminal Record Systems 11
- Criminal History Record Completeness and Disposition Reporting 12
- Standards for Security, Privacy, and Electronic Exchange of Fingerprints 15

The Ident Automation Strategic Plan: Critical Assumptions and Scenarios 17
- Assumptions About NFF/III Implementation and Criminal Justice Use 17
- Assumptions About Baseline Noncriminal Justice Use 19
- Assumptions About New Fingerprint Check Applications 21
  - Federal Agency Fingerprint Check Proposals 21
  - Other Fingerprint Check Proposals 23
- Assumptions About Response Time 26
- Assumptions About File Size 27
- Assumptions About Storage Requirements 29

Cost, Schedule, and Staffing Implications 31
- Illustrative Review of Ident Automation Costs 31
  - Computer Matcher Requirements 31
  - Building Construction Requirements 33
  - Impact on Ident Costs 33
- Composition and Training of Ident Workforce 36
- Technical and Schedule Risk 37

Tables

Tables *Page*

1. State Plans for III Participation 11
2. Impact of NFF/III Implementation on FY2000 Daily Criminal Justice Fingerprint Card Submissions 17
3. Projected Daily Noncriminal Justice Fingerprint Card Submissions, FY2000 Base Level 20
4. Projected Total Fingerprint Card Submissions per Day, FY2000 Base Level 21
5. Possible Additional Federal Fingerprint Check Requirements 23
6. Possible FY2000 Targets for Fingerprint Card Submissions 24
7. Range of Estimated Fingerprint Card Submissions Per Day, FY2000 26
8. Number of Computer Matchers Required by Year 2000, as a Function of Daily Fingerprint Submissions 32
9. Scenarios for Ident Fingerprint Volume, Staffing, and Office Complex Requirements, Year 2000 34
10. Scenarios for Ident Daily Fingerprint Volume, Response Time Matchers, and Cost 35

Boxes

Boxes	*Page*
A. Why Automated Fingerprint Checks?	2
B. A Year in the Life of a State AFIS	6
C. How the National Fingerprint File/Interstate Indentification Index (NFF/III) Will Work	7
D. Cal-ID: An Early Success Story	29
E. Ident Automation: A Necessary Risk	36

Figures

Figures	*Page*
1. Arrests Supported by Fingerprints in State Criminal History Files, 1989	5
2. Final Dispositions in State Criminal History Files, 1989	13
3. Automation of State Criminal History Records, 1989	13
4. State-by-State Percentages of Automated Criminal History Records and Final Dispositions, 1989	14
5. Total Volume of Fingerprint Cards Submitted to Ident by Type, 1981-90	18
6. Distribution of Fingerprint Cards Submitted to Ident by Type, 1990	19
7. Projected Volume of Fingerprint Cards Submitted to Ident, 2000	25
8. Projected Number of Ident Computer Matchers, 2000	31
9. Projected Number of Ident Personnel, 2000	34
10. Projected Illustrative Ident Automation Costs, Selected Items	35

Summary

Automated fingerprint identification and criminal history records are vital for effective law enforcement and criminal justice. These records also are increasingly used for a range of noncriminal justice purposes, such as background checks of applicants for employment, licenses, or security clearances. Fingerprint checks are essential to ensure positive identification, detect or deter persons using aliases or phony identification documents, and protect the civil liberties of arrestees, applicants, or employees.

Manual fingerprint and record systems are incapable of meeting today's needs for timely and accurate information. Many States and the Federal Bureau of Investigation (FBI) have made significant progress over the last decade in automating these systems. But the extent of automation and quality of records varies widely, and significant gaps in automation and record quality exist. Criminal justice activities are being hindered as a result. Proposed new national criminal record checks will be difficult or impossible to implement until further improvements are in place.

Several events have combined to make the needed improvements possible:

1. the extraordinary performance of automated fingerprint identification and computerized criminal history records systems that has been demonstrated at the Federal, State, and local levels;
2. the recognition that automated systems and improved record quality are needed to perform "instant" checks of criminal records, e.g., when booking and setting bail for arrestees;
3. the ongoing efforts to modernize the FBI's Identification Division (Ident), linked with a move of Ident from Washington, DC, to Clarksburg, West Virginia; and
4. the growing consensus among criminal justice officials on the National Fingerprint File/Interstate Identification Index (NFF/III) concept and proposals to enact the necessary interstate compact or Federal legislation.

The NFF/III would reduce the duplicate fingerprints and criminal history records currently received or maintained by Ident. Ident would maintain only one fingerprint card (or image) per offender per State and no criminal history records (except on Federal offenders), but would provide an index of all offenders. The NFF/III is, in principle, a sound concept for the Federal/State/local partnership in criminal fingerprint identification and criminal history record systems. The time and resources required to implement NFF/III are not yet known. The FBI and the Bureau of Justice Statistics (BJS) need to make a detailed assessment of implementation requirements.

Full NFF/III implementation requires, in addition to time and resources, agreement on uniform national rules for the interstate exchange of criminal history information—especially when such information is used for noncriminal justice purposes (e.g., employment and licensing). The rules should cover who can have access to what criminal history records for which purposes. An interstate compact is, in principle, a sound concept for enacting national rules. Questions remain, however, about the content, timing, and feasibility of a compact. The U.S. Attorney General and the FBI need to consult with State legislatures and governors, as well as Congress, to further refine the proposed compact, develop a ratification plan, and determine under what circumstances Federal legislation might need to be considered in lieu of a compact.

Criminal history record improvement must be an integral part of the NFF/III and Ident automation programs and may need to be included in an interstate compact or legislation. The FBI is requesting funds to eliminate a large backlog of unprocessed fingerprint cards and dispositions over the next 2 years, and to automate remaining active criminal history records over the next 4 years. The Federal Government is providing grant funds for State/local record quality and automation improvements in support of automated firearm purchaser check initiatives. Ident could develop a more comprehensive record quality program, including criminal history audits by or for State/local agencies and mandatory review and challenge procedures to protect the civil liberties of persons undergoing record checks. BJS and the Bureau of Justice Assistance (BJA) need to develop a detailed State-by-State record improvement and funding plan.

The NFF/III and modernization would enable Ident to improve its service and regain leadership in fingerprint identification. This will require extraordinary cooperation and support by the States, and substantial funds from the Federal Government.

The Ident modernization program is the most costly item on the Nation's criminal record improvement agenda—estimated at about $600 million in capital investment over the next 4 years, including the new building in West Virginia ($200 million) and its

automated equipment and systems ($400 million). Technical advances and design modifications may reduce costs, but the investment will still be large.[1]

The FBI has spent a year working on the strategic plan for the Ident automation program. It will be the basis for the design and procurement of the FBI's automated fingerprint identification and criminal record system. A well-executed strategic plan could ensure that the technical system meets the needs in a feasible, timely, cost-effective way.

The overall FBI technical strategy appears, qualitatively, to be sound. The Ident emphasis on the electronic scanning, transmission, processing, and storage of fingerprints is appropriate, even though the full transition from paper to electronic will take years. The emphasis on developing a common standard for the electronic exchange of fingerprints, rather than a generic fingerprint matching algorithm, is correct; this assures compatibility with all Federal and State/local automated fingerprint systems. The size of the planned

Box A—Why Automated Fingerprint Checks?

An automated fingerprint identification system (AFIS) permits law enforcement agencies to run far more fingerprint checks than are feasible with manual processing. The payoff is greatest when comparing latent prints (partial prints from a crime scene) against fingerprints of suspects or prior offenders already on file, and when comparing prints of a suspect against those of persons wanted, charged, or convicted for offenses committed in other jurisdictions.

Western Identification Network, Inc. (WIN) is a regional AFIS that serves the States of Alaska, California, Idaho, Nevada, Oregon, Utah, Washington, and Wyoming. Fingerprint check results from the first months of WIN operation highlight the value of automated checks:

- In Idaho, latent prints from a stolen and recovered police car were entered into the WIN AFIS, with no match indicated. A week later fingerprints of a suspect in an unrelated case were checked against the WIN database, resulting in a hit (a match between the latent print from the stolen car and the full fingerprint of the arrestee).
- In Utah, fingerprints from an unidentified deceased 20-year-old person were entered into the WIN AFIS, resulting in a match with the prints of a person in the Portland, Oregon, fingerprint file. Knowing the victim's identify led police to a suspect who was subsequently arrested on murder charges.
- In Washington State, latent prints from the rearview mirror of a vehicle at the scene of a rape were entered into the WIN AFIS, resulting in a fingerprint match and subsequent identification and arrest of a suspect.
- In Nevada, latent prints from the scene of a robbery and assault in Carson City were entered into the WIN AFIS. The victim received serious head injuries and could not identify or remember anything about the assailant, but the latent fingerprint check resulted in a match and subsequent arrest of a suspect in Virginia City.
- In Wyoming, special agents arrested three suspects in Cheyenne on drug charges. Two of the suspects claimed to be illegal aliens, but WIN AFIS searches identified them as repeat offenders with prior criminal records in Utah and Nevada.
- In Nevada, the Washoe County Sheriff's Office arrested an unknown person on charges of using stolen credit cards to obtain money from teller machines. A WIN AFIS search identified the suspect as a repeat offender with a prior criminal record in Oregon, which led in turn to an FBI record check indicating that the suspect was wanted by the U.S. Secret Service, State of North Carolina, and District of Columbia for fraud and weapons violations, and had arrests in seven States using multiple aliases.
- In Oregon, the State Police entered latent prints from a truck at the scene of an unsolved 1978 homicide into the WIN AFIS, resulting in a match with the prints of a person in the Washington State fingerprint file who was subsequently arrested.

SOURCE: Western Identification Network, Inc., 1990 and 1991.

[1]The impact of automation on operating costs is not known, although the FBI is assuming that labor productivity will increase by 50 to 100 percent, thus significantly reducing the cost per fingerprint check.

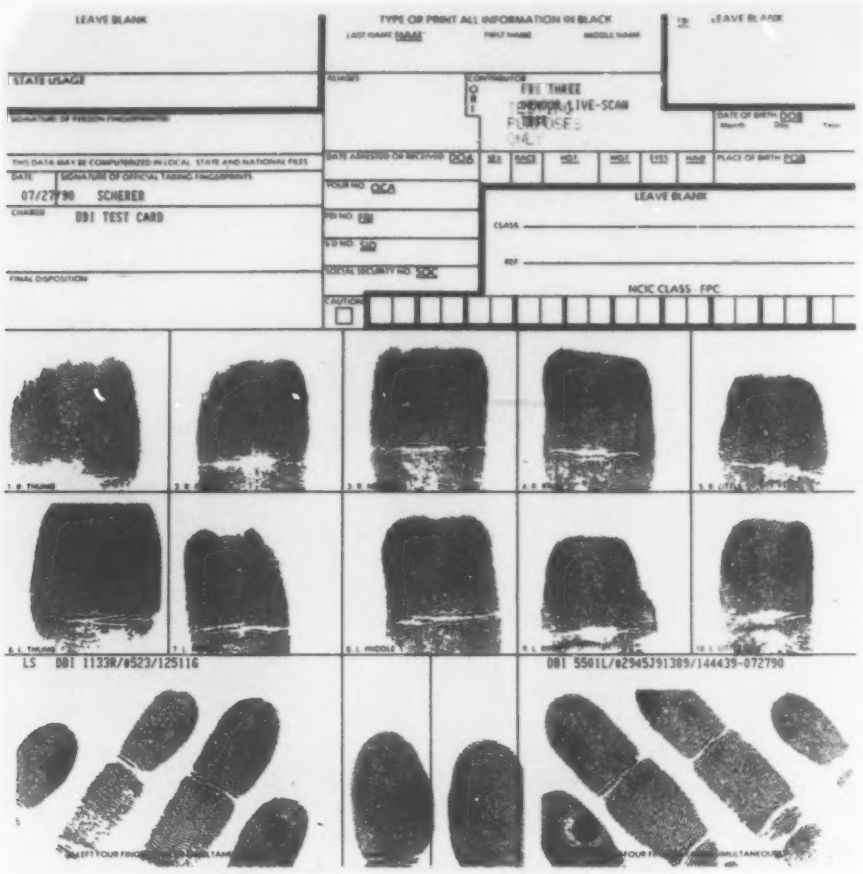


Photo credit: Federal Bureau of Investigation

A typical fingerprint card includes space for the rolled prints of each individual finger, flat prints of both thumbs, and flat prints of the left and right four fingers. The card includes space for the name and identifying information of the person being fingerprinted, the date and name of the official taking the fingerprints, and arrest and disposition information if applicable. The fingerprints in this sample were taken using a live scan fingerprint reader (using light or laser beams rather than ink). Trained operators can take live scan prints with a quality equal to or better than inked prints.

system is reasonable, although the projected file size and demand for fingerprint checks are still uncertain. The FBI should design the system to accommodate projected use plus some margin of error for unanticipated growth. States have found the greater risk to be underdesigning new automated fingerprint identification systems, with demand typically exceeding design capacity faster than expected.

Another potential payoff of Ident modernization is improved processing of latent fingerprints. Latent prints are single or partial fingerprints from door handles, walls, firearms, clothing, and other items found at or near the scene of a crime. The FBI needs to design its latent searchable file to complement similar files maintained by Federal and State/local criminal justice agencies. Many States report that old and/or difficult criminal cases have been solved due to latent matches that could not be conducted on a manual basis (see box A).

The FBI should analyze the tradeoffs among volume and type of fingerprint checks, file sizes, response times, technical design, cost, schedule, technical risk, number and type of employees, training needs, and building requirements. These analyses are under way and should be completed before the FBI procurement process proceeds further so that the results can be used

by the Administration and Congress in making decisions on system design and funding.

OTA's review suggests that the FBI could minimize automation cost by

1. ensuring that the NFF/III is implemented to the maximum extent possible concurrently with Ident modernization,
2. making realistic assumptions about the daily volume of new or expanded noncriminal justice fingerprint checks, and
3. adjusting the system design to defer or phase in capabilities that may not be needed right away.

These actions, combined with technical advances, could reduce the capital investment cost of Ident automation by several tens of millions of dollars over what would otherwise be required. The Administration and Congress may need to allocate equivalent funds for improvements in State/local automated identification and record systems to support NFF/III, and for Federal and regional automated identification systems that complement NFF/III.

The current Ident automation schedule is tight and allows little margin for error. Ident is proposing to procure a larger, more complex system than has been installed by even the largest States, yet in the same time frame as these States, and with the complications of moving to a new building hundreds of miles away from its current location in Washington, DC, relocating existing employees, hiring new employees, and training virtually all employees.

The move does offer the prospect of a more stable, higher quality Ident workforce, since salaries should be more competitive, living costs lower, and commutes shorter for employees living in the Clarksburg, West Virginia, area. (Ident employees who do not elect to move have been guaranteed continued FBI employment in the Washington, DC, area with no loss of pay.) The move should help Ident break with the past and establish a new, state-of-the-art facility with a reenergized workforce. The existing obsolete system will not be moved but instead will be phased out at the present location over a transitional period.

The FBI must skillfully use the design and procurement process to structure an advanced system with acceptable risk. Requests for vendor information before issuing the formal request for proposals, and benchmark or prototype tests during the selection process, as planned by Ident, will help ensure a successful procurement. The technical risk can be reduced and the schedule better maintained by procuring the best commercially available technologies (existing at the time of procurement), and conducting any remaining automated identification research and development (R&D) work on a separate, longer term schedule.

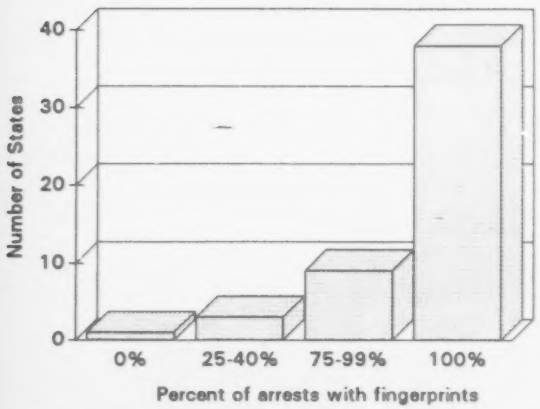
The U.S. Department of Justice agencies involved with criminal record systems and record quality improvement—the FBI, BJA, and BJS—have an opportunity to coordinate their efforts. Effective collaboration over the next 10 years could ensure that by 2000, the Nation will have a substantially automated and complete criminal identification and record system.

The Context for Ident Automation

There is widespread agreement among Federal, State, and local law enforcement officials that automation of the fingerprint identification process is essential to improve law enforcement and enhance criminal justice in the United States.[2]

Fingerprint identification is the most practical and widely accepted method for positive biometric[3] identification, and is likely to remain so for the foreseeable future.[4] It is used to establish the identity of persons arrested or who are otherwise involved with the criminal justice process (see figure 1). Criminal records tied to fingerprints are used to track criminal cases from booking through adjudication, and, where applicable, through sentencing, incarceration, probation, and parole. Many criminal justice decisions—e.g., charging, sentencing, and paroling—are based in part on a defendant's prior criminal record. Federal and State laws now require that repeat violent offenses and serious drug offenses carry longer, mandatory sentences with reduced opportunity for parole.

Figure 1—Arrests Supported by Fingerprints in State Criminal History Files, 1989



SOURCE: Bureau of Justice Statistics/SEARCH Group, Inc., 1991.

Fingerprints normally are taken by rolling the inked fingers over paper fingerprint cards that are then manually examined, processed, filed, stored, and exchanged. This is a time-consuming and labor-intensive process. Law enforcement agencies find, increasingly, that manual fingerprint identification is no longer workable. Resources required for manual fingerprint checks often exceed the staff and budgets available. Manual fingerprint checks can take too long for the law enforcement action required, particularly if a full fingerprint check must be conducted at the time of arrest, booking, or bail decisions. Manual comparison of prints from a crime scene with prints from a fingerprint file (known as a latent print search) is difficult and frequently impossible. Matching crime scene prints with those on file is like searching for the proverbial needle in a haystack—a job ideally suited for computers.

The Automated Fingerprint Identification System (AFIS) is a proven technology. AFIS is based on computer matching or comparison of the digitized physical identifiers from individual fingerprints (known as fingerprint minutiae).[5] Most fingerprint cards processed by computer are still rolled manually and physically distributed or exchanged. Pilot tests indicate that the live scanning of fingerprints (with lasers or light, not ink) and transmission in digital form are technically feasible.[6]

The majority of States have some form of AFIS or plan to implement an AFIS system (see box B). States have found AFIS checks to be much more accurate, faster, and more cost-effective than manual fingerprint

[2]See, for example, T.F. Wilson and P.L. Woodard, SEARCH Group, Inc., *Automated Fingerprint Identification Systems: Technology and Policy Issues*, NCJ-104342 (Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, April 1987); U.S. Department of Justice, Bureau of Justice Assistance (BJA), *Planning for Automated Fingerprint Identification Systems (AFIS) Implementation* (Washington, DC: U.S. Department of Justice, BJA, June 1988); National Crime Information Center Advisory Policy Board (NCIC APB), III Ad Hoc Subcommittee, Identification Services Task Group, *Identification Division Revitalization*, August 1989, available from the FBI.

[3]Unique human descriptors such as retina scans, voice prints, and fingerprints.

[4]For discussion of biometric technologies, See U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987); *Criminal Justice: New Technologies and the Constitution*, OTA-CIT-366 (Washington, DC: U.S. Government Printing Office, May 1988); and *Genetic Witness: Forensic Uses of DNA Tests*, OTA-BA-438 (Washington, DC: U.S. Government Printing Office, July 1990). Also see SEARCH Group, Inc., *Legal and Policy Issues Relating to Biometric Identification Technologies* (Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, June 16, 1989).

[5]See Wilson and Woodard, *Automated Fingerprint Identification Systems*, op. cit., footnote 2.

[6]Federal Bureau of Investigation (FBI), Identification Division, *Final Report of the Pennsylvania State Police/FBI Live-Scan Pilot Test*, Aug. 31, 1990, and *Final Report of the Internal Revenue Service/FBI Pilot Test of Live-Scan Fingerprint Cards*, May 31, 1990, both available from the FBI.

Box B—A Year in the Life of a State AFIS

California has a State-wide automated fingerprint identification system (AFIS), known as the California Identification System or Cal-ID. Cal-ID provides automated fingerprint and criminal record services to local, county, and State law enforcement and criminal justice agencies.

Cal-ID includes an AFIS database covering arrestees and offenders, and an Automated Latent Print System (ALPS) data base with a subset of the AFIS database that can be searched against latent prints from crime scenes.

1989 was a typical year in the life of Cal-ID. In that year, Cal-ID:

- included fingerprint minutiae (for thumbs only) on 6.26 million persons in the AFIS database;
- searched 295,949 criminal fingerprints against the AFIS database yielding 54,597 positive identifications (18.5 percent of searches);
- searched 362,188 civil fingerprints against the AFIS database yielding 14,758 positive identifications (4.1 percent of searches);
- included fingerprint minutiae (for 8 fingers) on 1.8 million persons in the ALPS database;
- searched 7,372 latent fingerprints against the ALPS database yielding positive identifications in 646 cases (8.8 percent of searches);
- identified suspects through latent searches in 32 homicide cases, 33 narcotics cases, 33 robberies, 92 grand thefts, 9 sex crimes, and 9 assaults.

SOURCE: California Department of Justice, *California Identification (CAL-ID) System Remote Access Network (RAN) Status Report: 1989-1990* (Sacramento, CA: California DOJ, Division of Law Enforcement, Bureau of Criminal Identification, 1990).

checks.[7] The FBI has its own custom-designed AFIS, known as the Automated Identification System (AIS); but the FBI's system is obsolete and incompatible with the AFIS systems used by the States. The average FBI fingerprint check time is 15 to 20 work days (mail delays can increase the average to 20 to 30 days) and is too slow for many criminal justice purposes.

The FBI's Ident revitalization program will upgrade the AFIS technology and make it compatible with State systems to provide a faster response.[8] This modernization is a part of Ident's planned move by 1995 from the J. Edgar Hoover Building in Washington, DC, to Clarksburg, West Virginia. State and local law enforcement and criminal justice agencies support the modernization of the FBI's fingerprint identification operations.[9]

The Ident modernization plan is known as the Integrated Automated Fingerprint Identification System (IAFIS), and provides for the electronic transmission, storage, and processing of fingerprints.[10] During the transition from paper to electronic formats, traditional paper fingerprint cards will be scanned and converted to electronic images. All processing and matching of fingerprint images by Ident will be done electronically, with verification by fingerprint examiners. Ident expects that a significant percentage of fingerprints will be received electronically during the early years of IAFIS operation, but that full electronic transmission will take many years to implement—primarily due to limited State/local funding.

Several related key issues—besides technical design and funding—can affect the modernization program's ability to improve the Nation's overall criminal identification and record system. The Administration and Congress may wish to include these topics as part of the Ident modernization plan:

- expeditious implementation of the NFF/III concept;
- enactment of an interstate compact or Federal legislation on criminal justice record systems;
- further improvement in criminal history record completeness and disposition reporting; and
- setting of standards for security, privacy, and electronic interchange of fingerprints.

[7]AFIS systems typically achieve 97- to 98-percent accuracy, compared with 75-percent accuracy for the old Henry system of manual fingerprint classification and comparison.

[8]FBI, *Automation Program for Identification Division Revitalization*, Aug. 30, 1990, available from the FBI.

[9]See minutes of relevant meetings of the National Crime Information Center Advisory Policy Board and SEARCH Group, Inc. Board of Directors, available from the FBI and SEARCH Group, Inc., respectively.

[10]For a detailed overview, see FBI, *Automation Program*, op. cit., footnote 8.

The National Fingerprint File/Interstate Identification Index (NFF/III) Concept

The States, the FBI, and others in the criminal justice community have long debated their roles in a national fingerprint identification/criminal history record system. The debate has addressed a range of options, from a fully centralized FBI role to the substantially decentralized system that exists today.[11] The criminal justice community generally supports the so-called NFF/III concept (see box C), in which the FBI's Ident would: 1) receive one fingerprint card per criminal offender per State (instead of several cards), 2)

Box C—How the National Fingerprint File/ Interstate Identification Index (NFF/III) Will Work

For a typical arrest situation, the NFF/III will work as follows, using San Diego, California, as an illustration:

- The arresting officer in the San Diego County Sheriff's Department brings the suspect to the sheriff's office for booking.
- The suspect is fingerprinted and interviewed, to obtain his/her name and other identifying information.
- The suspect's name and identifiers are entered into the San Diego County Sheriff's computerized criminal record system to see if the suspect has a prior local criminal history record. If the suspect's name matches a name already on file, the suspect's fingerprints are compared with the fingerprints on file to make positive identification.
- If the suspect's identity is verified through a fingerprint match, then the name and identifiers (including previously assigned criminal identification numbers) are checked against the California State Department of Justice (DOJ) criminal record system and the FBI's III to see if the person has a prior out-of-county or out-of-State criminal history record.
- If the suspect's name does not match a name already in the San Diego County Sheriff's criminal record file, then the suspect's fingerprints are searched against the local automated fingerprint identification system (AFIS) database to see if the prints match anyone using a different name. If a match occurs, the suspect can be positively identified at the local level.
- If the suspect's fingerprints do not match any prints in the San Diego AFIS, the suspect's prints are then transmitted to the California State DOJ in Sacramento for comparison against the larger State-wide AFIS database. If a match occurs, the suspect can be positively identified at the State level.
- If the suspect's fingerprints do not match any prints in the State-wide AFIS, the prints are then transmitted to the FBI's AFIS in Clarksburg, West Virginia, to be searched against the FBI's much larger fingerprint database (known as the NFF). (Prints might also be transmitted to a regional AFIS, such as the Western Identification Network, Inc., that serves California and several other Western States.)
- If an NFF match occurs, the FBI electronically notifies the California DOJ and San Diego Sheriff's Department of the suspect's true identify (including the FBI criminal identification number) that permits the requesting agency to query local and State criminal record systems and the III. The FBI updates the III to show that the suspect now has an arrest in California in addition to any other State(s) already listed. If no NFF match occurs, the FBI adds the suspect's fingerprints to the NFF, and adds the suspect's name and identifiers to the III.
- The FBI's NFF will contain one fingerprint per offender; States will submit, as a general rule, only the first fingerprint per offender per State.
- The FBI's III will list the State(s) in which each offender has a prior criminal record, but will not include the actual criminal record information, such as arrests and dispositions. (The exception will be Federal offender records available directly from the FBI.)
- When the NFF/III is fully implemented, criminal history record information on State offenders will be maintained and provided by the States—not the FBI. The traditional FBI rap sheet will cease to exist, but instead will be an electronic composite drawn from individual States (and the FBI for Federal offenders).

SOURCE: Office of Technology Assessment, Federal Bureau of Investigation, California Department of Justice, San Diego County (California) Sheriff's Department, 1990, 1991.

[11] See U.S. Congress, Office of Technology Assessment, *An Assessment of Alternatives for a National Computerized Criminal History System*, OTA-CIT-161 (Washington, DC: U.S. Government Printing Office, October 1982); and FBI, *Interstate Identification Index Phase Three Test Findings June-July 1987* (Washington, DC: Nov. 30, 1987) and *Interstate Identification Index Program: National Fingerprint File Operational Plan* (Washington, DC: July 10, 1990). Also see NCIC APB, *Identification Division Revitalization*, op. cit., footnote 2.

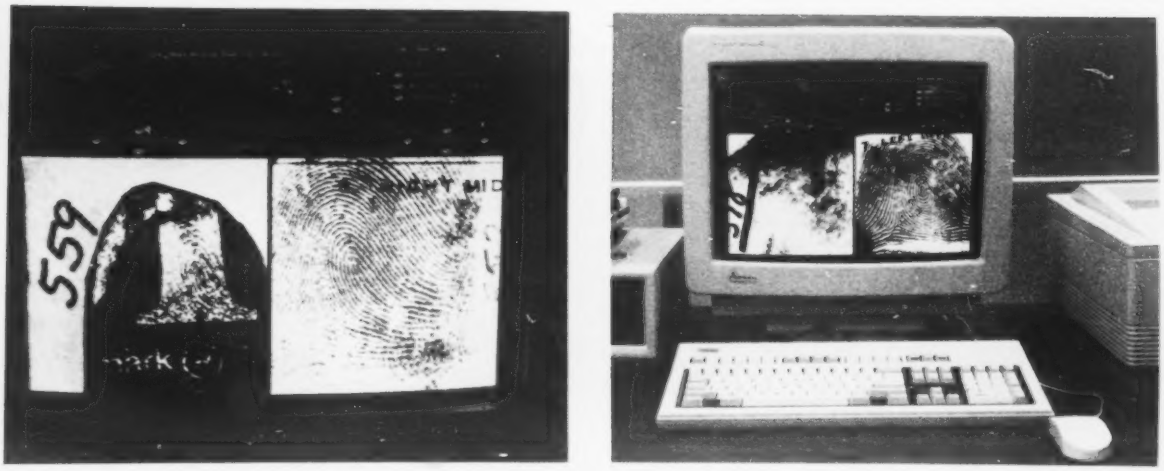


Photo credits: Federal Bureau of Investigation, 1991

An automated fingerprint identification system (AFIS) speeds up the matching of latent prints from crime scenes with prints of known offenders already on file. Latent prints are single or partial fingerprints from door handles, walls, firearms, clothing, and other items found at or near the scene of a crime. The AFIS computer compares the latent print with the large number of fingerprints on file and identifies any tentative matches. A fingerprint examiner then compares the prints on a computer screen to make the final match.

Left: A typical latent print on the left side of the screen is compared with a full fingerprint on the right.

Right: Latent and full prints are compared using a video display terminal and microcomputer keyboard. Print images are stored on optical disks.

retain no criminal history information on non-Federal offenders (except for basic identifiers such as date of birth and race), and 3) maintain an index (the III) of offenders with records in one or more States (but not the criminal history records themselves). The NFF/III is predicated on the basis that 60 to 70 percent of all offenders are repeat offenders.[12] These persons will already have a criminal history record based on positive fingerprint identification, and will have State and Federal identification numbers previously assigned. The out-of-State records of repeat offenders would be obtained from individual States by using III.

With full implementation of NFF/III, there would no longer be an FBI "rap sheet" per se, except for Federal offenders. Criminal history records on multi-State offenders would be compiled electronically by combining the criminal records from each State. Each entry into the III would be based on a positive fingerprint identification using the NFF.

Assumptions about NFF/III will affect the design of the Ident automation program. If fully implemented, the NFF/III concept should significantly reduce the number of criminal fingerprints submitted to the FBI. The FBI currently receives duplicate fingerprint cards for many offenders, either for repeat offenses within the same State or for charging, sentencing, and correctional actions on the same offender. In some States, the fingerprint cards are routed through a central source (usually the State identification or criminal records agency); in others, fingerprint cards are sent through multiple channels. Some State/local agencies do not send all fingerprints to the FBI, and some fingerprints received by the FBI are rejected as illegible. The net result is an incomplete fingerprint system.

Implementation of NFF/III should considerably reduce the FBI's criminal history recordkeeping. The majority (about 80 percent) of criminal history records maintained by Ident duplicate records in State criminal justice repositories. Only about 20 percent of State offenders have multi-State records.[13] Most record activity is within the home States. The quality (completeness and accuracy) of Ident records is a major

[12]FBI estimate, 1991. The FBI has assumed, for planning purposes, that 65 percent of offenders have multiple arrests.

[13]FBI estimate, 1991.

problem, because of disposition backlogs within Ident and incomplete disposition reporting by States. States face a major challenge as it is in maintaining high-quality criminal history records on their own. Trying to maintain complete and up-to-date records on about 24 million persons at the national level is even more difficult.

For the NFF/III to work, each State should have

1. a central Statewide fingerprint identification and criminal records repository;
2. centralized reporting of prints and records to this repository;
3. single-source reporting, meaning that only one agency per State—presumably the central repository—submits prints to the FBI;
4. a computerized criminal history records system so that III responses can be provided electronically within seconds;
5. adherence to uniform rules for the interstate exchange of criminal history records for non-criminal as well as criminal justice purposes; and
6. a basic AFIS capability (either at the State repository or accessible via a regional network) so that fingerprint checks can be processed expeditiously.

Full NFF/III implementation thus would reduce the demands on the FBI and the Ident automation program. The NFF/III should significantly reduce the number of criminal fingerprints submitted to the FBI; it also should greatly reduce the number of criminal fingerprints and criminal history records maintained by the FBI. Rejection or failure of the NFF/III, on the other hand, would put greater demands on the FBI, since Ident would need to process multiple duplicate fingerprint cards and maintain a large number of State criminal history records, as it does today. With partial NFF/III implementation, demands on the FBI would fall somewhere in between. In this case, the FBI would, in effect, provide computer and recordkeeping support for those States that did not have their own capabilities to participate in NFF/III. Only a few States appear able to assume full NFF/III responsibilities by 1995.[14] Most States are not likely to fully participate in NFF/III for 5 to 10 years or longer, unless additional resources and incentives are provided.

Twenty-one States currently participate in III (not, however, in the NFF). These States account for about 80 percent of the Nation's criminal history records and fingerprints.[15] The FBI is still maintaining duplicate records and fingerprint cards for these States. The FBI and Florida are conducting a pilot test of the full NFF/III concept. Florida is submitting only one fingerprint card per offender to Ident, and most Florida criminal history records are being consolidated in Florida. Florida is primarily responsible for responding to III inquiries, but the FBI continues to be responsible for residual Florida records maintained by Ident.

A successful Florida test would be a major step toward full NFF/III implementation. It would help provide direction for the FBI and the other 20 States that are III participants. Full NFF/III implementation will take several years. A 1991 FBI survey found that 25 States plan to participate in NFF by 1995, and 7 additional States by 2000. A recent FBI update found that State participation in NFF may proceed more slowly, with as few as 9 States by 1995 and 20 States by 2000:[16]

- 9 to 10 States by 1995, representing no more than 20 percent of total criminal fingerprint card submissions;
- 20 to 25 States by 2000, representing no more than 50 percent of fingerprint submissions; and
- all States by 2008.

Interim Florida pilot test results confirm the benefits of III but also confirm the problems and complexities of full NFF implementation that are likely to stretch out the schedule.

The III, in contrast, is a proven concept, and State participation is likely to progress faster. A 1990 FBI survey (updated in 1991) found that 14 States, in addition to the current 21, plan to participate in III by the end of 1993, and 4 States after 1993 (see table 1). Eight other States plan to participate but have no definite schedule, and three States have no plans or schedule. The FBI believes that full III participation is possible by 1995 or 1996.

Congress and the FBI may wish to include NFF/III implementation as an integral part of Ident automation. If so, then several further actions are necessary. First, an interstate compact or Federal legislation would be

[14]According to estimates of the FBI and the NCIC Advisory Policy Board, Identification Services Subcommittee.

[15]Based on the number of fingerprint cards submitted by the States to the FBI.

[16]FBI estimate, presented at the July 29, 1991, OTA workshop on the Ident automation program.

Photo credits: Oregon State Police, 1991

The National Fingerprint File Interstate Identification Index (NFF/III) would facilitate the accurate and speedy identification of persons with prior out-of-State criminal history records. The NFF/III could be used for a variety of purposes—from reviewing the criminal records of arrestees when setting bail, to checking firearm purchasers for felony convictions, to screening employment and licensing applicants for disqualifying criminal records.

Right: The name and identifying information of a prospective handgun purchaser are entered into a local police computer system for checking against local, State, and national criminal record files—including the III.

Left: The thumbprints of a prospective handgun purchaser are compared with fingerprints of prior offenders in a regional AFIS—which in the future could be connected to the NFF. Here, a fingerprint examiner verifies a tentative match between the thumbprints of a purchaser with those of a prior offender, in order to establish positive identification.

required to establish uniform operating rules and designate responsibilities needed to make the NFF/III work, especially for noncriminal justice use of criminal history records. Second, this would require that the States be willing and able to change State laws on noncriminal justice use to be consistent with an interstate compact or legislation. Third, a detailed assessment of current and projected State capabilities to support NFF/III would be needed to ensure full implementation in an agreed-to time frame.[17] This assessment should include consideration of regional AFIS networks for smaller States, such as the Western Identification Network that serves Alaska, California, Idaho, Nevada, Oregon, Utah, Washington and Wyoming.[18] The FBI and BJS could collaborate with the States in preparing a detailed State-by-State NFF/III implementation plan.

Fourth, Federal grant programs for State/local criminal justice record systems should be reviewed to ensure that NFF/III implementation is given a priority. Congress included a provision in the Crime Control Act of 1990 requiring that 5 percent of Federal criminal justice block grants be used to improve State/local criminal justice record systems. This could amount to about $20 million per year starting in fiscal year 1992, or perhaps $100 million total through fiscal year 1996 or $200 million through fiscal year 2001 (possible milestones for significant NFF/III implementation).[19] Fifth, the States would need to make up the difference between their NFF/III cost and any Federal assistance through tax revenues and user fees.

[17]Two recent surveys provide useful information, but are not by themselves sufficient for developing a detailed NFF/III implementation plan. See SEARCH Group, Inc., *Survey of Criminal History Information Systems*, NCJ-125-620 (Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, March 1991), and FBI, survey of State needs and capabilities for fingerprint identification and criminal history record checks, 1991, results available from the FBI.

Table 1—State Plans for III Participation[a]

State	Planned participation
Alaska	1991 (1 State)
Arkansas, Illinois, Kansas, Kentucky, Nebraska, Nevada, New Hampshire, North Dakota, South Dakota, Utah, Washington, West Virginia, and Wisconsin	1992-1993 (13 States)
Indiana, Maine, Mississippi, Vermont	After 1993 (4 States)
Alabama, Arizona, Hawaii, Iowa, Maryland, New Mexico, Oklahoma, Rhode Island	No schedule (8 States)
Louisiana, Massachusetts, Tennessee	No plans to participate (3 States)

[a]Twenty-one States already participate.

SOURCE: Federal Bureau of Investigation, 1990, 1991.

Interstate Compact or Federal Legislation on Criminal Record Systems

If the NFF/III is fully implemented, and Ident no longer maintains State criminal history records, the interstate exchange of criminal justice information could be impeded in the absence of uniform rules. Agreement on uniform national rules for the use of criminal records for nonjustice purposes is especially important because about half of the requests for Ident fingerprint/criminal record checks historically are for such purposes—about 30 percent from Federal agencies and 20 percent from State/local agencies. Ident currently handles these requests without regard for widely varying State laws on noncriminal justice dissemination. Once the information is submitted to the FBI, it is subject to Federal—not State—laws. State laws differ on what types of criminal justice information (e.g., arrest record, convictions only) can be disseminated for specific purposes (e.g., employment, licensing). Current State laws would make national noncriminal justice record checks incomplete and perhaps unworkable, since the information provided would be a "patchwork quilt" with some of the patches missing.

Representatives of many of the State criminal justice agencies agree on a proposed solution to the noncriminal justice problem—that the laws of the requesting (or recipient) State should take precedence. For instance, if California requested a criminal history check for employment or licensing purposes on someone who had a prior criminal record in Arizona and Texas, records would be used by California in accordance with its law—not the laws of Arizona or Texas. Similarly, if a Federal agency such as the Defense Investigative Service (DIS) requested a record check on a defense contractor employee with a prior record in Maryland and New York, the State records would be provided to DIS for use in accordance with Federal law.

During the 1980s, two major criminal justice advisory groups—the National Crime Information Center Advisory Policy Board (NCIC APB, chartered under the Federal Advisory Committee Act to advise the FBI) and SEARCH Group, Inc. (a not-for-profit State consortium on criminal justice information policy)—and the FBI developed policy proposals for the interstate exchange of criminal history information.[20] These initiatives included rules on criminal justice as well as noncriminal justice use of criminal records and specified State and Federal responsibilities for NFF/III implementation and oversight. The three proposals are similar in many respects but have a few differences.

The SEARCH Group and FBI policy proposals covered both criminal justice and noncriminal justice use of NFF/III, while the NCIC APB proposal was limited to noncriminal justice purposes. All three proposals included new advisory groups, but they differed in how these groups would be formed and would operate. The NCIC APB proposed that a new advisory group be responsible only for noncriminal justice uses of NFF/III, with criminal justice activities continued

[18]For further information, see *Bits & Hits*, a newsletter published by the Western Identification Network, Inc., 9343 Tech Center Drive, Suite 250, Sacramento, CA 95826.

[19]States correctly point out that the 5-percent set-aside is not new money, and must be transferred from other State/local criminal justice purposes. BJA/BJS have not yet issued guidelines on qualifying uses of the grant monies set aside.

[20]For three interstate compact proposals, see SEARCH Group, Inc., "Interstate and Federal-State Compact on the Exchange of Criminal History Records," July 20, 1989; FBI, "Interstate Compact on the Exchange of Criminal History Records," working draft, Aug. 4, 1989; and NCIC APB, Interstate Identification Index Subcommittee, "Interstate and Federal-State Compact on the Exchange of Criminal History Records for Noncriminal Justice Purposes," final draft, Nov. 16, 1989, and revised final draft, Dec. 6, 1990. The FBI Director approved the NCIC APB draft on May 16, 1991, and forwarded it to the U.S. Attorney General for action.

under the NCIC APB's purview.[21] The FBI withdrew its proposal and supports the NCIC APB approach. SEARCH Group, Inc., has also endorsed the APB proposal compact, even though some SEARCH members prefer a broader approach.[22]

The NCIC APB, SEARCH, and the FBI have endorsed an interstate compact to establish common procedures for the interstate exchange of criminal justice information. The FBI Director has approved the APB compact and forwarded it to the U.S. Attorney General for action. Any compact would have to be ratified by State legislatures and Congress. If Congress decides to make NFF/III implementation a part of Ident automation, and if an interstate compact proves difficult to ratify, Federal legislation could substitute for a compact. The FBI could ask the National Conference of State Legislatures, National Governors Association, National Criminal Justice Association, and other appropriate organizations to survey the views of State legislators and governors on criminal record policy. The survey could include questions about the content, timing, and feasibility of a compact, and preferences for a compact versus legislation. The compact may need to more explicitly addressed, for example, the completeness of criminal history records exchanged and the procedures by which persons can review and challenge adverse record check results.

The FBI will have to make major decisions over the next few months on the strategic direction of the Ident automation program. If the FBI bases its automation plans on full NFF/III implementation, it would have to ensure that binding operating rules and responsibilities would be agreed to on a timely basis—whether through interstate compact or Federal legislation. It will take time to adopt and ratify an interstate compact. A possible objective could be to begin the interstate compact ratification process during the 102d Congress. This would give the FBI a basis for planning, identifying any substantive problems with the proposed compact, and possibly formulating Federal legislation should an alternative to the compact be needed.

Criminal History Record Completeness and Disposition Reporting

Congress and criminal justice study groups, most recently in relation to the identification of felons attempting to purchase firearms, have emphasized the importance of record quality in criminal justice information systems.[23] Incomplete or inaccurate criminal history records can reduce the effectiveness of law enforcement and the criminal justice process, and jeopardize individual rights. Record quality problems can frustrate fully informed charging and sentencing decisions in criminal cases, and make it difficult to conduct accurate criminal record checks on applicants for government employment or licenses, child care providers or teachers, firearms purchasers, and the like, where authorized or required by law.

The FBI did not, until 1990, distribute criminal history records for State/local noncriminal justice purposes when the record showed an open arrest (i.e., no disposition listed) more than 1 year old. The FBI now distributes such records, although with a warning that applicants should be presumed innocent if no disposition is listed and should be given an opportunity to challenge record information if used against them.[24] This has not eliminated concern over possible civil rights violations if incomplete records are used for licensing and employment decisions. If records without dispositions are not used at all, on the other hand, some convicted offenders would be licensed or hired. Complete and accurate records are the only solution to this dilemma.

The FBI continues to have problems with missing dispositions, either because they are not reported by the States or because the FBI lags in entering the reported dispositions into the criminal history records. A significant percentage of reportable dispositions (roughly 30 to 50 percent) are never provided to the FBI. Ident currently has a backlog of about 2.5 million unprocessed

[21]For further discussion, see NCIC APB, "Interstate and Federal-State Compact," op. cit., footnote 20.

[22]See SEARCH Group, Inc., resolution dated July 18, 1991, available from SEARCH Group, Inc., 7311 Greenhaven Drive, Suite 145, Sacramento, CA 95831.

[23]See U.S. Congress, Office of Technology Assessment, *Automated Record Checks of Firearm Purchasers: Issues and Options*, OTA-TCT-497 (Washington, DC: U.S. Government Printing Office, July 1991); U.S. Department of Justice, Office of Justice Programs, *Attorney General's Program for Improving the Nation's Criminal History Records and Identifying Felons Who Attempt To Purchase Firearms*, NCJ-128131 (Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics, March 1991); U.S. Department of Justice, Task Force on Felon Identification in Firearm Sales, *Report to the Attorney General on Systems for Identifying Felons Who Attempt To Purchase Firearms* (Washington, DC: U.S. Department of Justice, Assistant Attorney General for Justice Programs, October 1989).

[24]FBI, Fingerprint Contributor Letter 90-4, "FBI Identification Division Services: One-Year Rule," Aug. 9, 1990.

dispositions. Full implementation of NFF/III would help solve this problem by getting the FBI out of the business of collecting and maintaining criminal history information—including dispositions—except for Federal offenders, and placing the responsibility for record quality with the States.

Until that can be done, magnetic computer tape can be used for disposition reporting, and additional staff can be assigned to reduce the FBI disposition filing backlog. Several States are submitting dispositions on magnetic tape, with good success. The Attorney General has approved an FBI request for additional resources to eliminate the disposition backlog over the next 2 years, but this is a small fraction of total missing dispositions.

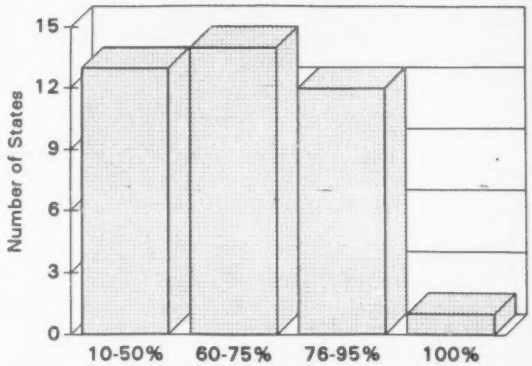
Disposition reporting is also a problem at the State level, although the States are a step closer to the sources of dispositions (police, prosecutors, courts, correctional officials) than the FBI. Many States have taken various actions over the last decade to improve disposition reporting and record quality and automation. Surveys estimate overall disposition reporting and record automation rates of 60 to 70 percent, with some States achieving higher rates and others lower (see figures 2 and 3).[25] Whatever the actual rates, there is still room for improvement.

Both OTA and the Attorney General's Task Force on Felon Identification in Firearm Sales concluded that record quality problems are a major barrier to implementing automated checks of firearms purchasers.[26] Federal law prohibits convicted felons from obtaining or possessing firearms. If criminal history records are missing disposition information, then it is difficult or impossible to determine whether a person arrested for a felony offense was actually convicted and thereby disqualified from purchasing a firearm.

In recognition of the importance of improving criminal history record quality, the Attorney General authorized the expenditure of $9 million per year for 3 years (FY91, FY92, FY93) in BJS/BJA grants to the States for criminal record system improvements related to record quality. These relatively modest sums appear to be having a beneficial impact on the States. Several States report that, in these times of tight State budgets, even a few hundred thousand dollars in "new" money can fund projects that are critical to improving record quality. Typical projects include software upgrades to automate disposition reporting, record quality audits, and conversion of manual records to computerized formats.

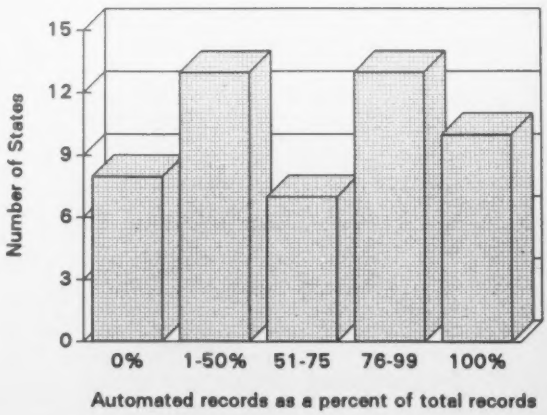
In addition, Congress included in the Crime Control Act of 1990 a 5-percent set-aside of Federal criminal

Figure 2—Final Dispositions in State Criminal History Records, 1989



SOURCE: Bureau of Justice Statistics/SEARCH Group, Inc., 1991.

Figure 3—Automation of State Criminal History Records, 1989

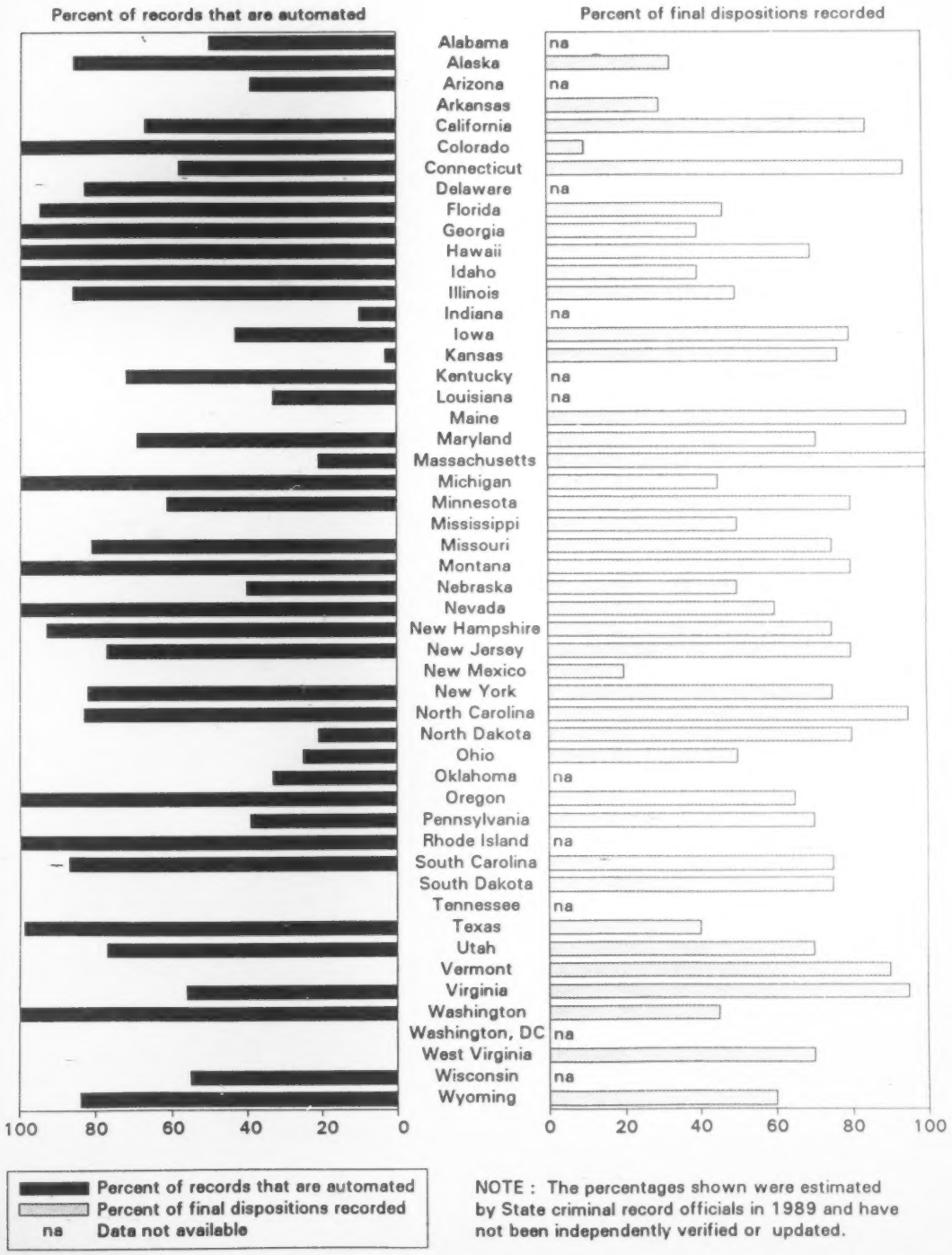


SOURCE: Bureau of Justice Statistics/SEARCH Group, Inc., 1991.

[25]SEARCH Group, Inc., *Survey of Criminal History Information Systems*, op. cit., footnote 17. Also see OTA, *Automated Checks of Firearm Purchasers*, op. cit., footnote 23.

[26]See OTA, *Automated Checks of Firearm Purchasers*, op. cit., footnote 23; U.S. Department of Justice, *Attorney General's Program*, op. cit., footnote 23; and *Report to the Attorney General*, op. cit., footnote 23.

Figure 4—State-by-State Percentages of Automated Criminal History Records and Final Dispositions, 1989



NOTE : The percentages shown were estimated by State criminal record officials in 1989 and have not been independently verified or updated.

SOURCE: Office of Technology Assessment and Bureau of Justice Statistics/SEARCH Group, Inc., 1991.

justice block grant funds (an estimated $20 million per year, starting in FY92) for criminal record system improvement related to record quality. This action also reflected the recognition that automated record checks of firearms purchasers require improved record quality. The Senate-passed version of the Violent Crime Control Act of 1991 includes authorization for $100 million in additional Federal funds for State/local record quality and automation improvements needed to support automated firearm purchaser checks. This Act also establishes a nationwide minimum disposition reporting standard of 80 percent. This standard, if implemented, would modestly improve the national average and dramatically upgrade reporting in States with the lowest disposition levels (see figure 4).

Further record quality improvement actions could be included in the Ident automation program. For example, Ident could develop and implement a fingerprint identification and criminal history record audit program. The FBI's National Crime Information Center (NCIC) already conducts audits of State/local "hot file" record systems (e.g., the wanted persons and stolen vehicles files).[27] Each State is audited about every 3 years on a rotating basis. The audits include compliance with NCIC procedures, related training programs, and record quality of selected files. The record quality audits include a comparison of the entries in the NCIC national files with the corresponding entries in State/local files based on a random sample of records from each file. Incomplete or erroneous entries and other discrepancies are discussed with the appropriate State/local criminal justice officials, along with remedial actions that may be necessary.

Ident could conduct or require similar audits of State/local fingerprint and criminal history record systems. The audits themselves could be carried out by State/local auditing agencies, rather than Ident, with Ident providing guidelines and reviewing the results. The audits could include compliance with Ident procedures to be developed for use with the NFF/HI and automated systems, within the framework of an interstate compact or statute. If the interstate transmission of fingerprints and criminal history records uses the NCIC telecommunications network, then compliance with NCIC operating procedures would likely be audited as well. The audits also might include training programs, as they do for the NCIC hot files.

Development and implementation of an Ident record quality program need not wait on completion of Ident modernization or NFF/III. The program could be in place within 1 to 2 years, if it were assigned high priority and given adequate resources.[28]

An accurate and responsive criminal records system today requires an automated system. Both the FBI and many States have gaps in the automation of their criminal history records (see figure 4). Ident still maintains about one-third of its records in manual format. As part of an effort to upgrade criminal record systems in support of automated firearm purchaser checks, the Attorney General has proposed funds to begin to computerize Ident's remaining manual records on active criminal offenders.[29] The FBI estimates, however, that it will take 4 years to convert these records. The BJS/BJA grant and set-aside funds can be used for similar upgrades at the State/local levels. These improvements will help facilitate the interstate exchange of criminal history information for a wide variety of purposes.

Standards for Security, Privacy, and Electronic Exchange of Fingerprints

Fingerprint identification files and criminal history records maintained by Ident are perhaps even more sensitive than the hot files (e.g., on wanted persons and stolen vehicles) maintained by NCIC. NCIC has developed procedures to protect the NCIC network from unauthorized use, sabotage, and other physical, technical, and personnel security breaches. Only authorized law enforcement and criminal justice personnel may access NCIC. The NCIC APB places a high priority on a secure, tightly controlled NCIC network. For this reason, the APB expressed reservations about proposals to permit gun dealers (and other noncriminal justice personnel) direct NCIC access. Noncriminal justice users may obtain NCIC information, but only for authorized purposes and with access provided through authorized law enforcement or criminal justice personnel. In addition, NCIC has procedures to protect the privacy of NCIC record information, including III and criminal history records transmitted over NCIC, by limiting their dissemination to authorized persons.

[27]See NCIC audit reports for specific States, available from the FBI.

[28]Full implementation of State-by-State audits and training could take longer, but the FBI should be able to define, develop, and initiate a record quality program within 2 years.

[29]Records on older, inactive offenders will not be automated.

297-920 O - 91 - 3

Similar security and privacy standards should be included in the Ident automation program. If Ident uses the NCIC telecommunications network for fingerprint and record transmission, as planned, the NCIC standards would apply as they already do today to III/Ident criminal history record dissemination. Security and privacy should be explicitly included in any Ident audit program that may be developed. Ident should consider issuing binding Federal regulations, or seeking legislation if necessary, to mandate procedures for persons to review and challenge the results of criminal history record checks used against them. This is especially important so long as a significant percentage of records are missing dispositions but are nonetheless disseminated and used for noncriminal justice purposes. Review and challenge procedures also could be included in an interstate compact; most States have such procedures, although the specifics vary. State record repositories could provide user agencies with two copies of the record check results, one for the agency and one to be passed on to the applicant, or a copy could be sent directly to the applicant.

The FBI recognizes the need to design the Ident automation program to be technically compatible with State/local fingerprint identification and record systems.–NFF/III implementation depends on the exchange of fingerprints and criminal history records among the States/localities and the FBI. Electronic transmission is essential for timely, cost-effective exchange. Technical standards for the electronic exchange of documents such as criminal history records are widely used in the computer and telecommunications industries. These standards are incorporated into State/local systems that interface with the NCIC network and the National Law Enforcement Telecommunications System.

All States use different formats for criminal history records, whether manual or automated. This is a presentation problem and not a technical matter, and all of the formats contain adequate information for most criminal justice purposes. Nonetheless, efforts to standardize criminal history record formats are needed. Standardized formats could be important for proposed new record checks, such as automated firearm purchaser checks using III. The Virginia State Police, for example, have found that out-of-State criminal history records can be obtained through III in 10 to 15 seconds. But because of differing record formats (and quality), it may take 15 to 20 minutes or longer to interpret the out-of-State records. This is longer than the State Police can reasonably hold gun dealers on the telephone line awaiting a record check on firearms purchasers. Initial approval or disapproval decisions sometimes are based on whether there is a III "hit" (a match between the name of the gun purchaser and a name listed in the index of criminal offenders), not on the content of the criminal record. III entries may eventually be flagged to indicate persons with felony convictions, thus eliminating the need to review detailed criminal history records when checking firearm purchasers. But review of the actual records would still be needed for many other kinds of noncriminal justice record checks.

As for fingerprint transmission, the FBI is supporting an initiative by the National Institute of Standards and Technology (NIST) to develop standards for electronic transmission of fingerprint images.[30] Numerous vendors and users are participating in the NIST standard-setting activity. The standard is intended to permit the electronic capture of fingerprints (through live scanning with video or laser units)[31] and transmission of the digitized print images to local, State, or Federal agencies with automated fingerprint identification systems. The receiving agency could store the prints on magnetic or—more typically—optical media, display the prints on a computer screen, and print the fingerprints out on paper if needed. Multiple copies of fingerprints could easily be sent in later transmissions of the electronic images. This process would make obsolete the time-consuming and error-prone rolled ink copies and the mail or hand delivery required for duplicate (or triplicate) manual fingerprints.

Finally, the FBI has determined that standardized fingerprint search algorithms, which would permit the exchange of fingerprint minutiae among different systems, are not needed. A standard or generic, nonproprietary search algorithm compatible with all major vendor proprietary systems would be difficult to develop. Successful implementation of the NFF/III and Ident automation depends not on a generic search algorithm but, instead, on standards for the electronic transmission of digitized fingerprint images and related information.[32]

[30]For an update on progress to date, see FBI, "Proceedings of the May 1991 Workshop on the Fingerprint Image Transmission Standard," cosponsored by the FBI and NIST.

[31]Scanning can also be used to capture fingerprints of deceased crime victims.

[32]AFIS vendors and users, the FBI, and the NIST have concluded that a generic algorithm is not feasible or necessary.

The Ident Automation Strategic Plan: Critical Assumptions and Scenarios

The FBI has spent the last year working on a strategic plan for the Ident automation program. The strategic plan will provide the basis for the design and procurement of the FBI's automated fingerprint identification and criminal record system. A quality strategic plan will help ensure that the technical system meets well-defined needs in a realistic, timely, cost-effective way. Therefore careful congressional consideration of the FBI's planning process is needed. The FBI faces several challenges in developing a strategic plan and making key assumptions about

- NFF/III implementation and criminal justice use,
- baseline noncriminal justice use,
- new fingerprint check applications,
- response time,
- file size, and
- storage requirements.

Assumptions About NFF/III Implementation and Criminal Justice Use

The plan depends on assumptions about the implementation of NFF/III. If the NFF/III can be fully implemented, including enactment of an interstate compact or Federal legislation, then the daily volume of criminal fingerprints received by Ident could be reduced by as much as 50 percent or more from what it would otherwise be. This reduction would likely be the case even if there were an increase in the underlying level of criminal activity.

Ident received about 17,900 State and local criminal fingerprint cards per day in fiscal year 1990.[33] (All estimates of daily fingerprint card submissions assume 250 workdays per year—365 days less weekends and holidays.[34]) This number would increase to about 24,000 cards per day in 2000, assuming a basic underlying annual growth rate of 3 percent and no implementation of NFF/III (see table 2).[35] The volume would reach 29,200 cards per day in 2000, assuming 5-percent annual growth. (Use of the term "cards" includes fingerprint images as well, to the extent electronic submissions replace paper cards by 2000.) If the NFF/III is phased in over a 10-year period, then this expected growth rate would be more than offset by reductions in State/local criminal fingerprint card submissions. The maximum reduction would be about 65 percent of the base in any given year after full NFF/III implementation, since roughly that proportion of criminal offenders are repeat offenders whose records (and fingerprints) should already be on file. Thus State/local fingerprint card submissions could decline from 18,000 per day in fiscal year 1990 to about 8,400 per day in fiscal year 2000 with full NFF/III and 3-percent underlying annual growth, or to about 10,200 per day assuming 5-percent growth. If the NFF/III is half implemented in fiscal year 2000, perhaps a more realistic scenario, the reduction would be 30 to 35 percent of the baseline growth. Under this scenario, State/local submissions would decline marginally to about 16,800 cards per day in fiscal year 2000 with 3-percent underlying growth, or increase modestly to 20,400 cards per day with 5-percent growth.

Table 2—Impact of NFF/III Implementation on FY2000 Daily Criminal Justice Fingerprint Card Submissions

	Cards per day		
	State/local	Federal	Total
FY90 base (no growth)	17,900	700	18,600
With 3% a.g.			
With no NFF/III	24,100	940	25,040
With half NFF/III	16,800	940	17,740
With full NFF/II	8,400	940	9,340
With 5% a.g.			
With no NFF/III	29,200	1,140	30,340
With half NFF/III	20,400	1,140	21,450
With full NFF/III	10,200	1,140	11,340

a.g. = annual growth.

SOURCE: Office of Technology Assessment, 1991.

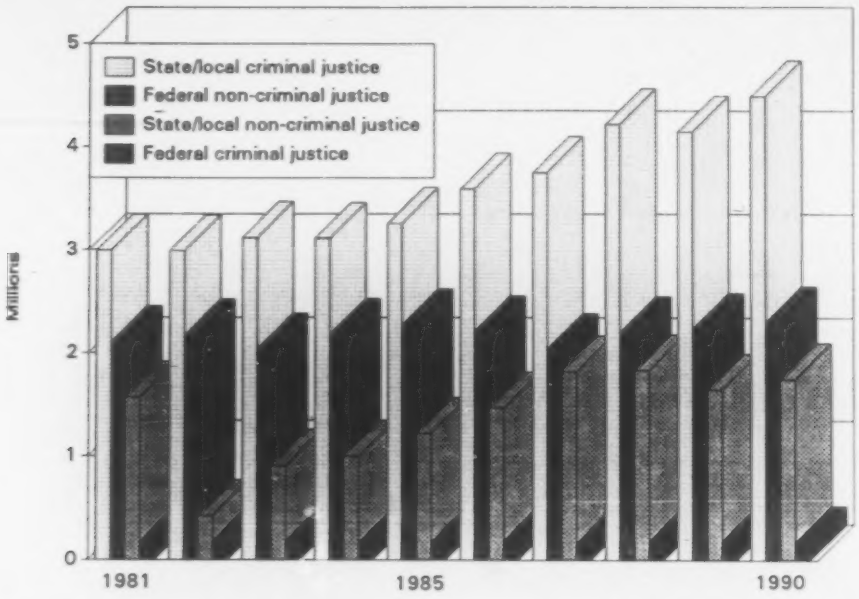
Ident receives a small number of Federal criminal fingerprint cards—about 700 per day in fiscal year 1990. This number would increase to perhaps 940 per

[33] 4.48 million cards divided by 250 workdays per year.

[34] Ident currently operates with a full day shift and one-half evening shift Monday through Friday (except holidays), and with a skeleton staff nights, weekends, and holidays to handle emergency requests and system maintenance. Ident assumes that the same basic staffing pattern will be used with a fully automated system.

[35] State/local criminal fingerprint card submissions increased about 2 percent/year for FY81-85, but 4 percent/year for FY86-90.

Figure 5—Total Volume of Fingerprint Cards Submitted to Ident by Type, 1981-90



SOURCE: Federal Bureau of Identification, 1991.

day at an assumed annual growth rate of 3 percent, and to 1,140 per day at 5-percent annual growth (which is far greater than the historical rate[36]—see figure 5). The total combined (Federal plus State/local) daily criminal fingerprint card volume thus could range from a low of about 9,000 with full NFF/III to a high of about 25,000 with no NFF/III and 3-percent underlying growth (see table 2). With 5-percent growth, the total combined criminal fingerprint volume could range from about 11,000 to 30,000 cards per day, again depending on the extent of NFF/III implementation.[37]

The FBI's crime statistics indicate that total criminal arrests grew by about 3 percent per year from 1980 through 1989, and that serious crime arrests grew by about 2 percent annually.[38] Thus an assumed 3-percent baseline growth rate for the next decade should cover likely increases in criminal fingerprint card submissions generated by criminal activity. A 5-percent baseline growth rate would allow for some further increase in the underlying crime rate or in fingerprint submissions for other reasons (e.g., new types of fingerprint checks, old fingerprints not submitted previously).

Since criminal fingerprints account for about half of the total number of fingerprints received by Ident (figure 6), full NFF/III implementation should translate into at least a 25-percent reduction in daily fingerprint activity, other things being equal. Also, full NFF/III implementation should result in a large reduction—as much as 90 to 95 percent—in the size of the computerized criminal history file maintained by Ident.[39] Whether and when this reduction will be realized is unclear, since it assumes that States will take full responsibility for all of their own records, including those currently maintained by Ident.

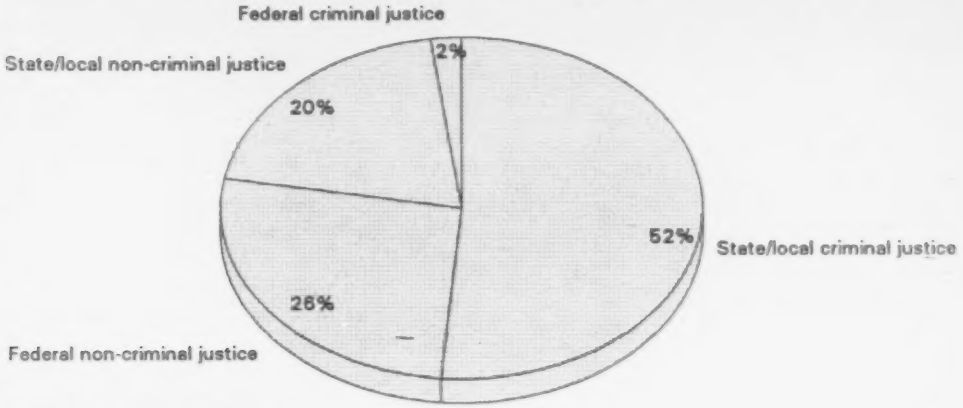
[36]The number of Federal criminal fingerprint card submissions grew only slightly over the last decade, fluctuating between 661 and 742 cards per day.

[37]The FBI questions whether full NFF/III implementation will be realized in the foreseeable future, and has concluded that 50-percent implementation is the best that can reasonably be expected by 2000.

[38]See U.S. Department of Justice, FBI, *Crime in the United States: Uniform Crime Reports 1989* (Washington, DC: U.S. Government Printing Office, August 1990), p. 176.

[39]Even with full NFF/III implementation, the FBI is likely to retain responsiblity for some older, less active or inactive records that are not maintained by the States.

Figure 6—Distribution of Fingerprint Cards Submitted to Ident by Type, 1990



SOURCE: Federal Bureau of Identification, 1991.

Assumptions About Baseline Noncriminal Justice Use

The plan also depends on assumptions about growth in current noncriminal justice uses of the Ident system. Noncriminal justice fingerprint checks account for about half of all Ident fingerprint card activity. Full implementation of NFF/III might result in a small reduction in noncriminal fingerprint submissions to Ident, since a State's own fingerprint files would occasionally have the relevant fingerprint, eliminating the need to forward a print to the FBI. However, this reduction is likely to be more than offset by underlying growth in noncriminal justice fingerprint checks.

The total number of requests for noncriminal justice fingerprint checks received by Ident from State and Federal agencies has varied widely, but has shown little net change over the last 10 years—the number was about 3.7 million in 1981 and 4.1 million in 1990 (see figure 5). Ident believes, however, that growth has been artificially restrained due to policy changes and increases in FBI fees charged for noncriminal justice fingerprint checks.[40]

The number of requests for Federal noncriminal justice fingerprint checks received by Ident grew only slightly during the 1980s, from 2.1 million (about 8,400 per day) in fiscal year 1980 to 2.3 million (about 9,200 per day) in fiscal years 1989 and 1990. Most of these are for employment and security purposes. Federal agency officials expect no significant baseline growth during the 1990s, since the Federal civilian workforce is unlikely to grow, and the Federal defense workforce may actually shrink.

The Defense Investigative Service (DIS) conducts background investigations for Department of Defense security clearances (on military, civilian, and industrial defense personnel). DIS conducts about 800,000 to 900,000 national agency checks per year, of which 400,000 include a name check and 500,000 include both a name and a fingerprint check. Little or no growth in such checks is likely during the 1990s since any increases in investigative requirements should be offset by reductions in total personnel. The Office of Personnel Management (OPM) conducts background investigations on Federal civilian employees (including some civilians employed by the Department of Defense). OPM requests about 250,000 to 300,000 criminal record checks per year, including name and fingerprint checks. The volume of checks roughly corresponds to the personnel turnover rate.[41] OPM anticipates no significant change in baseline turnover rates or fingerprint check volumes during the 1990s (new

[40]In January 1990, the FBI established a user fee of $14 per fingerprint check for Federal employment applications, matching the fee previously established for fingerprint checks on State/local employment and licensing applications. In March 1990, the FBI raised the State/local employment and licensing fingerprint check fee to $20. In October 1990, the FBI raised the State/local fee to $23 per fingerprint check, and the Federal fee to $17 per check. The FBI believes that the noncriminal justice demand for fingerprint checks will rebound; however, the price elasticity of demand is unknown.

[41]Estimated to be 12 percent of 2.2 to 2.4 million employees.

agency-specific fingerprint check requirements are considered separately).

The Immigration and Naturalization Service (INS) conducts criminal record checks, including fingerprint checks, on about 1 million persons per year who are seeking to become permanent U.S. residents (legal aliens) or naturalized citizens, or who are seeking asylum (primarily refugees). The baseline total has increased slightly during the 1980s, with the exception of a temporary larger increase (or bulge) due to an amnesty program. INS expects the 1990s to be similar, but with some increase in the base growth rate (due to higher immigration), possibly augmented by another temporary increase in 3 to 8 years when some of those granted amnesty seek naturalization. INS also runs about 220,000 fingerprint checks per year on persons who are apprehended at port-of-entry inspection stations or by the U.S. Border Patrol (Ident counts these as Federal noncriminal justice, although they obviously have a law enforcement dimension).

DIS, OPM, and INS collectively account for about 90 percent of all Federal noncriminal justice fingerprint checks. The composite baseline estimates project no significant growth during the 1990s. Federal noncriminal justice fingerprint card submissions would grow from 9,200 per day in fiscal year 1990 to 10,200 per day in fiscal year 2000, assuming a 1-percent growth rate (see table 3), or 11,200 per day in fiscal year 2000 with a 2-percent growth rate (sources of growth above the base are discussed later). The assumed 1- to 2-percent annual baseline growth rate for the next decade should be adequate, since historical growth has averaged 1 percent over the last decade, and no net increase in Federal personnel or contractors is likely (again, new fingerprint check requirements are considered separately). The INS base might increase by as much as 4 to 5 percent per year by fiscal year 2000. But since DIS and OPM (accounting for about 60 percent of the Federal base) are likely to show very little if any baseline growth, a 2-percent overall growth rate should be able to accommodate INS needs. A 3-percent growth rate would provide an additional margin for any unanticipated new fingerprint check requirements.

Table 3—Projected Daily Noncriminal Justice Fingerprint Card Submissions, FY 2000 Base Level

	Cards per day
Federal:	
FY90 base (no growth)	9,200
With 1% a.g.	10,200
With 2% a.g.	11,200
With 3% a.g.	12,360
State/local:	
FY90 base (no growth—use FY88 peak year)	7,200
With 2% a.g.	8,800
With 3% a.g.	9,700
With 5% a.g.	11,700
Total:	
FY90 base	16,400
Federal at 1% a.g., State/local at 2% a.g.	19,000
Federal at 2% a.g., State/local at 3% a.g.	20,900
Federal at 2% a.g., State/local at 5% a.g.	22,900
Federal at 3% a.g., State/local at 5% a.g.	24,060

a.g. = annual growth.

SOURCE: Office of Technology Assessment, 1991.

State/local noncriminal fingerprint card submissions also increased slightly during the 1980s, from 1.6 million (about 6,400 per day) in fiscal year 1980 to 1.7 million (6,800 per day) in fiscal year 1990. Ident believes that demand was suppressed due to significant fee increases. The peak year was fiscal year 1988, when State/local submissions reached 1.8 million (7,200 cards per day). Setting data for fiscal years 1989 and 1990 aside, the annual growth rate between fiscal years 1980 and 1988 was about 2 percent. Using the peak year fiscal year 1988 figure as the starting point for fiscal year 1990, State/local submissions would reach 8,800 per day in 2000 with 2-percent annual growth, 9,700 with 3-percent growth, or 11,700 with 5-percent growth. This gives a noncriminal justice base range of about 19,000 to 24,000 cards per day in fiscal year 2000 (see table 3).

The combined base (criminal and noncriminal), assuming full NFF/III implementation, is about 29,000 to 34,000 fingerprint cards per day (see table 4). This means that the fiscal year 1990 level of 34,000 cards per day could be adopted as the fiscal year 2000 base level, although this figure would not allow much if any margin for new fingerprint check applications. Without NFF/III, the projected fiscal year 2000 volume would be 45,000 to 53,000 cards per day. With NFF/III at 50-percent implementation, the fiscal year 2000 volume would be 38,000 to 44,000 cards per day.

Table 4—Projected Total Fingerprint Card Submissions Per Day, FY2000 Base Level

	No NFF/III		Half NFF/III		Full NFF/III	
	3% a.g.	5% a.g.	3% a.g.	5% a.g.	3% a.g.	5% a.g.
Criminal justice:						
State/local	24,100	29,200	16,800	20,400	8,400	10,200
Federal	940	1,140	940	1,140	940	1,140
Noncriminal justice:						
State/local	9,700	11,700	9,700	11,700	9,700	11,700
Federal	10,200[a]	11,200[b]	10,200[a]	11,200[b]	10,200[a]	11,200[b]
Totals	44,940	53,240	37,640	44,440	29,240	34,240

a.g. = annual growth.
[a] = With 1% a.g.
[b] = With 2% a.g.

SOURCE: Office of Technology Assessment, 1991.

Assumptions About New Fingerprint Check Applications

Federal Agency Fingerprint Check Proposals

New applications could push the daily fingerprint volume above the baseline growth projections. Some possible criminal and noncriminal (also known as civil) applications include INS naturalizations (civil); U.S. Border Patrol and INS apprehensions (criminal); checks on U.S. Census Bureau census takers, Federal Aviation Administration airport employees, and U.S. Postal Service employees; U.S. Secret Service investigations (criminal); and International Police Organization (Interpol) investigations (criminal). Other possibilities (discussed later) are fingerprint checks of firearms purchasers, license applicants, child care providers, teachers, and financial and securities industry officials.

INS projects a possible increase in naturalizations starting in about 3 years and continuing for a 5-year period. This increase will depend on how many aliens granted amnesty apply for U.S. citizenship when eligible. INS estimates that up to 400,000 additional applicants could apply per year, resulting in about 1,600 more fingerprint checks per day (for roughly fiscal years 1995 to 1999).

The U.S. Border Patrol would like to expand fingerprint checks on aliens apprehended at illegal border crossing points. The Patrol intends eventually to check everyone apprehended—about 1 to 1.2 million persons per year (or about 4,800 checks per day)—but does not intend to use Ident for the primary fingerprint checks. The Patrol needs an initial response within minutes, and plans to use live scanned single fingerprints compared against a fingerprint file of illegal aliens who are serious repeat offenders.

The file size will be much smaller than State or Federal criminal fingerprint files, in order to ensure rapid response using low-cost live scan equipment. The Patrol is targeting repeat serious offenders (e.g., those smuggling drugs, guns, and persons), not aliens who are merely trying to get into the United States for jobs. The Patrol does not have the resources, prosecutors, or jails to follow up on more than a small percentage of illegal entries—thus the need to focus on the most serious offenders. When the initial fingerprint check shows a hit, the Border Patrol plans to run secondary checks against State and Federal criminal fingerprint files. The same approach is being considered for the INS Inspection Service, which makes about 2.4 million apprehensions per year (in addition to Border Patrol apprehensions).

The Border Patrol and INS inspections combined could generate over 3.4 million fingerprint checks by 2000. But these will be checked against INS, not FBI, fingerprint files. The number of followup checks against State and possibly Ident files might double. This would mean an increase from about 220,000 full checks in fiscal year 1990 (100,000 Border Patrol, 120,000 INS inspections) to perhaps 440,000 in fiscal year 2000—a net increase of 220,000. The net impact on Ident might be in the range of 900 additional fingerprint checks per day.

The U.S. Census Bureau normally has little need for fingerprint checks—perhaps 1,000 per year on Census

employees (these are counted in the OPM totals). But in decennial census years, the Census Bureau must screen up to 2 million applicants for temporary census taker jobs. The Census Bureau could use name checks as the primary criminal records screening tool, with fingerprint checks reserved for those with some indication of a criminal record or for otherwise questionable applicants. Based on its 1990 experience, the Census Bureau expects that about 15 percent of all applicants will have some kind of criminal record (based on a name hit) and one-fifth of these (3 percent of the total) will have a disqualifying record. Fingerprint checks may be needed on between 3 percent and 15 percent of applicants, spread over the 18 months to 2 years preceding the 2000 census. This would translate into 30,000 to 150,000 additional fingerprint checks per year (assuming 2 million applicants), or about 115 to 575 checks per day, for those 2 years.

Using name checks for applicant screening raises civil liberties questions, however, if applicants are not given the opportunity to challenge adverse findings. Name checks might, in addition, miss criminals using phony identification. Should the Census Bureau decide to request fingerprint checks on all census taker applicants (and if it can afford them), an additional 1 million fingerprint checks per year (about 4,000 per day) for 2 years would be needed.

The Federal Aviation Administration (FAA) has been directed to develop a plan for conducting criminal history record checks on all employees and applicants with unsupervised, unrestricted access to airport operations (AOA access).[42] The FAA is evaluating its options. An estimated 650,000 persons have airport identification badges,[43] but many (e.g., parking lot, restaurant, and gift shop employees) do not have AOA access. Assuming 500,000 persons with AOA access and a 15-percent annual turnover rate, about 75,000 new employee record checks per year would be needed. One plan under consideration is to run name-checks on all current employees, and fingerprint checks on those with a name check hit plus all new employees. This would translate into about 150,000 fingerprint checks the first year (75,000 on current employees, assuming 15 percent have a name hit, plus 75,000 new employees), and 75,000 (or about 300 per day) each year thereafter.

Name checks may not be sufficient for AOA access employees, given the high risk and cost of security breaches, as well as civil liberties concerns. If the FAA decided to run fingerprint checks on all other AOA-access employees, say over a 2-year period, then roughly 210,000 additional checks per year (840 per day) would be needed for 2 years. If the FAA decided to run fingerprint checks on all new AOA-access employees at the time of hiring and all current AOA-access employees on, say, a biannual basis, then an additional 325,000 checks per year (1,300 per day) would be needed on a continuing basis.

The U.S. Postal Service is planning to conduct new fingerprint checks on an estimated 60,000 to 100,000 applicants and employees per year. If implemented, this plan would mean 240 to 400 more fingerprint checks per day.

The U.S. Secret Service already has its own AFIS capability and criminal fingerprint file, and does not depend on Ident for many of its fingerprint checks. In order of priority, the Secret Service would prefer to run fingerprint checks against: 1) the Secret Service file, 2) regional or State files relevant to a particular investigation, and 3) the Ident file. Ident automation presumably would increase Secret Service demand for Ident fingerprint checks, but the impact on overall Ident volume is likely to be insignificant. The Secret Service believes, nonetheless, that access to the new Ident system is essential for all Federal criminal justice agencies, and that funding should be provided for the peripheral equipment and terminals needed to ensure such access.

Interpol provides an organizational link between foreign and U.S. law enforcement agencies. The U.S. Interpol office handles about 10,000 to 11,000 cases per year, of which about 20 percent require fingerprint checks by the FBI and/or States. This case level has been stable, with some short-term variations during tourist seasons, major political or sporting events, and world political and military situations. The volume of record checks might slowly increase, as other nations become more automated. But even if FBI fingerprint checks were run on all current cases (quadrupling the number of checks), the impact on Ident would be minimal (about 40 more checks per day).

The potential impacts of the possible additional Federal fingerprint checks discussed thus far are summarized in table 5. The projected increase is highest in fiscal year 1999, ranging from 3,380 to 8,240

[42]Includes aircraft, maintenance areas, fuel depots, runways, and taxiways.

[43]Airport, U.S. carrier, and foreign carrier personnel.

additional cards per day. The projected increase in the base level is much less—1,480 to 2,640 cards per day continuing after fiscal year 2000.

Assuming full NFF/III implementation, the fiscal year 2000 target could be increased from 34,000 cards per day (the high-end baseline growth) to 43,000 cards per day to cover these proposed new Federal fingerprint check applications. The 43,000 level would provide a cushion of about 5,000 to 6,000 cards per day for other new Federal (and perhaps State) applications after fiscal year 2000 (in non-Census years). This cushion seems adequate, especially if operational and financial conditions limit the demand for new fingerprint checks regardless of the FBI's capability. Federal officials indicate, for example, that funding for large-scale additional fingerprinting is by no means assured.

Other Fingerprint Check Proposals

Other proposals include running fingerprint checks on firearm purchasers, driver's license applicants, child care (or senior care) providers, teachers, and financial and securities officials. The efficacy and cost-effectiveness of these proposals have not been established. Detailed examinations of firearm purchaser check proposals have concluded that point-of-sale fingerprint checks are not feasible for the foreseeable future. Even the most optimistic forecast for Ident automation does not envision response times of less than hours—much longer than the seconds or minutes needed for point-of-sale checks. Point-of-sale fingerprint checks against criminal identification files would be very expensive. The limited evidence available suggests that the percentage of ineligible firearms purchasers that could be detected only through fingerprint checks (i.e., those using aliases or phony identification) may be very small.[44] Name checks may suffice, with fingerprint checks reserved for secondary verification when needed.

The firearm purchaser fingerprint check proposal points up the need for comprehensive research on the efficacy and cost-effectiveness of fingerprint checks for noncriminal justice purposes. The use of fingerprint checks needs to be rigorously compared with the use of name checks, or initial name checks plus secondary fingerprint checks, when: 1) the base rate of criminal

Table 5—Possible Additional Federal Fingerprint Check Requirements
(thousands per day)

Agency	Possible checks	Remarks
INS naturalizations	1.6	FY95-99
INS Inspection Service apprehensions	0.4	Continuing
U.S. Border Patrol apprehensions	0.5	Continuing
U.S. Census Bureau census takers	0.1-4.0	FY1999-2000
FAA Aviation Security employees	0.3-1.3	Continuing
U.S. Postal Service	0.2-0.4	Continuing
U.S. Secret Service	Negligible	
Interpol	Negligible	
Total increased base (INS inspections, Border Patrol, FAA, Postal Service)	1.4-2.6	Continuing
Increased base plus peak load (starting FY95)		
FY95 (+ INS Naturalizations)	3.1-4.2	
FY96 (+ INS)	3.1-4.2	
FY97 (+ INS)	3.1-4.2	
FY98 (+ INS)	3.1-4.2	
FY99 (+ INS, Census)	3.4-8.2	
FY2000 (+ Census)	1.8-6.6	
After FY2000	1.5-2.6	

SOURCE: Office of Technology Assessment, 1991.

[44]See OTA, *Automated Record Checks of Firearm Purchasers*, op. cit., footnote 23; Oregon State Police, *Study of Retail Firearm Sales and Concealed Handgun Licensing in Oregon* (Salem, OR: Oregon State Police, Criminal Investigative Division, 1990).

activity in the population being checked is very low, and 2) applicants or purchasers have an opportunity to challenge record checks that result in disapproval (as is the case with "instant" record checks of firearm purchasers at the point of sale).[45]

The use of name checks for many job applicants raises civil liberties questions, since applicants may not be told of the results or given an opportunity to challenge unfavorable findings. Name checks may be better suited for license applicants, who, like firearm purchasers, presumably are given notice and the opportunity to challenge adverse actions. Name checks may, on the other hand, miss persons using phony identification, and this risk must be carefully weighed. Consideration of each proposal for name or fingerprint record checks should involve a careful balancing of benefits against costs and risks.

Other potential sources of increases in the number of fingerprint checks are stimulation of additional demand for checks due to the convenience of electronic transmission, inclusion of some juvenile fingerprints in the State/local fingerprint submissions, and submission of an estimated 10 million State/local criminal prints held by State fingerprint repositories and not included in the FBI file.[46] The stimulation of demand depends, in part, on the efficacy and cost-effectiveness of electronic fingerprint checks. The target of 43,000 cards (paper or electronic) per day could accommodate perhaps a 5-percent stimulation of total demand (all purposes) after fiscal year 2000, in lieu of (but not in addition to) the additional margin for new applications previously identified.

The submission of juvenile prints, presumably for serious offenders, is an unresolved policy issue. The volume and timing of such submissions are unknown. Juvenile offenders (under 18 years of age) accounted for about 640,000 serious arrests in 1989, which would translate into about 2,500 fingerprint checks per day if all arrests were checked.[47] The 43,000-cards-per-day target probably could accommodate phasing in serious juvenile offender submissions by 2000, assuming that a high percentage are repeat offenders and would have fingerprints already on file. At a 3-percent annual growth rate, serious juvenile offenses would reach about 900,000 in 2000. If 35 percent were new offenders, an additional 310,000 fingerprint checks per year (1,200 per day) would be needed.

Table 6—Possible FY2000 Targets for Fingerprint Card Submissions[a]
(in thousands per day)

Criminal justice:	
State/local base with	
3% a.g. and full NFF/III	8.4
Federal base with 3% a.g.	1.1
Federal new applications (continuing):	
INS inspections	0.4
INS Border Patrol	0.4
Interpol/U.S. Secret Service	Negligible
State/local supplemental:	
Juvenile offender submissions	1.2
One-time criminal card submission of 1.7 million over 5 years (and then allows margin for demand stimulation, other new applications, or NFF/III slippage)	1.4
Subtotal	12.9
Noncriminal justice:	
State/local base + new applications with	
5% a.g.	11.7
Federal base with 2% a.g.	11.2
Federal new applications (continuing):	
FAA security	1.3
U.S. Postal Service	0.4
Federal supplemental:	
One-time civil card submissions (including	
INS naturalizations FY95-99):	1.6
Census FY1999-2000 (and then allows margin for other new Federal or State/local applications and demand stimulation)	4.0
Subtotal	30.2
Total FY2000	43.1
Plus State/local noncriminal justice base with additional 4-5% a.g. (9-10%/year total growth)	6.0
Grand total FY2000 high growth	49.1
Plus State/local criminal justice base with additional 2% a.g. (5%/year total growth) and half (rather than full) NFF/III	12.0
Grand total FY2000 high growth/half NFF/III	61.1

a.g. = annual growth.
[a] With full NFF/III implementation unless otherwise indicated.
SOURCE: Office of Technology Assessment, 1991.

[45]Only 1 to 2 percent of firearms purchasers, for example, appear to have disqualifying criminal records, and perhaps 10 to 15 percent have any kind of record. See OTA, *Automated Record Checks of Firearm Purchasers*, op. cit., footnote 23. In contrast, 60 to 70 percent of arrestees, on the average, will have a prior criminal record.

[46]Typically, such prints are not included in the FBI file becuase the State repository did not receive an extra fingerprint copy to forward to the FBI, or the FBI rejected a fingerprint card as illegible.

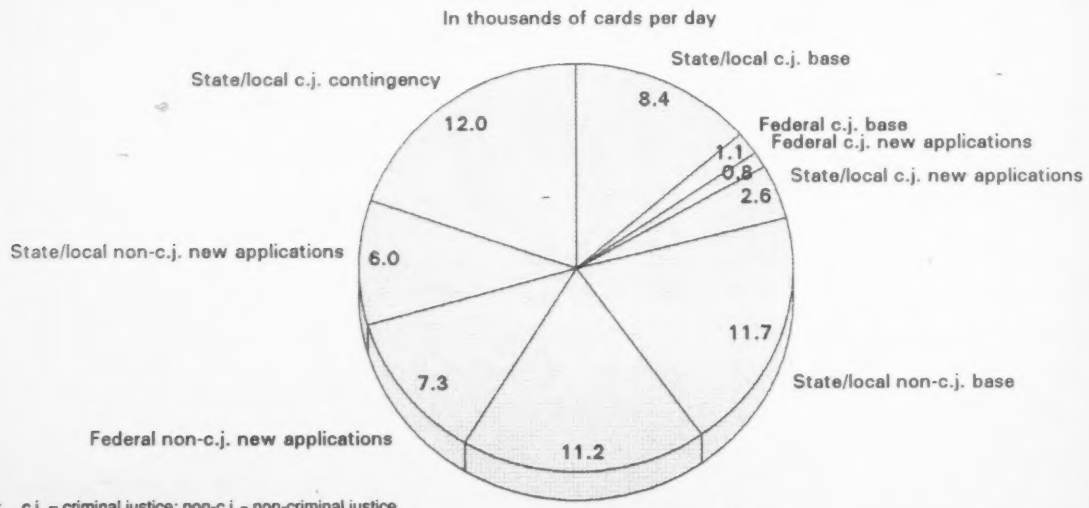
[47]See U.S. Department of Justice, *Crime in the United States*, op. cit., footnote 38, p. 182. Serious arrests include murder, nonnegligent manslaughter, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson.

The 43,000-print target could not handle submission of the estimated 10 million previously unfiled cards unless submissions were stretched out over many years; even 10 years would be tight, at 1 million cards per year (4,000 per day). The 10-million estimate, however, may be questionable.[48] The FBI has estimated that the actual number of unfiled prints on new persons (with no prints on file from prior arrests) is about 1.7 million (of the 10 million). This figure, spread over 5 years, would result in an increase in yearly card submissions of 340,000 (or about 1,400 cards per day). States should be able to identify most repeat offenders by first running name checks against State criminal history files and the III and then making a positive identification at the State level. This procedure would reduce or eliminate the need for FBI fingerprint checks on repeat offenders.

The remaining major area of uncertainty is the rate of growth due to fingerprint checks of license applicants, financial and securities officials, child care providers, and teachers, and other new State/local noncriminal justice applications (whether pursuant to State or Federal law). The FBI has surveyed all States concerning projected noncriminal justice applications. The initial survey results suggested a year 2000 daily volume of noncriminal justice fingerprint checks at 50 percent or more above FBI expectations. Subsequent validation and adjustment of the survey results indicate that the original FBI estimate (37,000 cards per day) is still reasonable. Using OTA's analytical framework, the FBI estimate is equivalent to assuming a 9 to 10 percent (rather than 3 or 5 percent) per year increase in State/local noncriminal justice fingerprint checks. This equates to an additional 6,000 to 7,000 checks per day.[49]

The total daily volume target could be increased to about 49,000 or 50,000 per day in 2000 (see table 6), which should allow for substantial baseline growth, significant new applications, and a healthy margin for contingencies and perhaps some slippage in NFF/III implementation beyond fiscal year 2000. If NFF/III is assumed to be half (rather than fully) implemented in fiscal year 2000, and baseline growth in State/local criminal justice use is assumed to be 5 (rather than 3) percent, an additional 12,000 checks per day would be needed. The total fiscal year 2000 daily volume target

Figure 7—Projected Volume of Fingerprint Cards Submitted to Ident, 2000



NOTE: c.j. = criminal justice; non-c.j. = non-criminal justice.
See table 6 and accompanying text for detailed explanation.

SOURCE: Office of Technology Assessment, 1991.

[48]The 10 million includes some percentage of the 400,000 illegible fingerprint cards previously returned by the FBI to the States each year, plus an unknown number of cards never submitted. Many of these cards are, however, for repeat offenders who already have prints on file in State repositories and/or Ident.

[49]At 10-percent annual growth, the FY90 State/local noncriminal justice base of 7,200 cards per day would increase to 18,674 cards per day in FY2000, compared with 11,700 cards per day at 5-percent annual growth—an increase of 7,000 cards per day.

Table 7—Range of Estimated Fingerprint Card Submissions Per Day, FY2000

	OTA-1[a]	OTA-2[a]	OTA-3[a]	OTA-4[b]	OTA-5[c]	OTA-6[c]
Criminal justice	11,000	13,000	13,000	25,000	34,000	50,000
Noncriminal justice	23,000	30,000	36,000	36,000	36,000	50,000
Total	34,000	43,000	49,000	61,000	70,000	100,000

[a] Full NFF/III implementation.
[b] Half NFF/III implementation.
[c] No NFF/III implementation.

NOTE: See text for explanation of OTA scenarios.

SOURCE: Office of Technology Assessment, 1991.

would then be about 61,000 fingerprint cards (see table 6 and figure 7). At 49,000 cards per day for full NFF/III implementation and 61,000 cards per day for half NFF/III implementation, the OTA and FBI projected totals are virtually identical, although arrived at using different methodologies.[50]

OTA has identified six scenarios for fingerprint card submissions (see table 7). The OTA-1, OTA-2, and OTA-3 scenarios assume full NFF/III implementation; the OTA-4 scenario assumes half NFF/III implementation. The OTA-5 and OTA-6 scenarios assume no NFF/III implementations. The OTA-1 scenario assumes no major new fingerprint check applications beyond what can be accommodated in the baseline growth. The OTA-2 scenario provides a margin for some new applications. The OTA-3, OTA-4, and OTA-5 scenarios provide margins for substantial additional baseline growth and new fingerprint check applications, assuming full, half, and no NFF/III implementation, respectively. The OTA-6 scenario assumes a much greater than expected growth in fingerprint checks with no NFF/III implementation, and reflects the unverified results of the FBI's user survey.[51]

Assumptions About Response Time

The plan must make assumptions about response or turnaround time for conducting FBI fingerprint checks. The current Ident system takes an average of 15 to 20 days to process fingerprint checks. Including mail delays, response time to the user can average 20 to 30 days. Many users claim total end-to-end response time can take 45 to 60 days (routinely, according to OPM), especially if the fingerprint cards must pass through several organizational levels. The FBI assumes a 2-hour criminal justice and 24-hour noncriminal justice response time, on the average, for the new system. Criminal justice checks would be given priority over noncriminal justice checks during peak periods. And the 2-hour criminal justice response would apply only to electronic (not paper) fingerprint submissions which are likely to account for only a minority of total submissions through the 1990s.

Most noncriminal justice fingerprint checks may require only about 5 to 10 days, even with a new automated system. If fingerprint checks could be consistently done this fast, the checks would no longer be the bottleneck in many employment and licensing clearances. OPM and DIS officials—two of the largest noncriminal justice users of Ident—indicate that a 5- to 10-day response time would be adequate for the purposes of Federal civilian and military (including defense contractor) screening. A faster turnaround would provide little if any advantage since other aspects of background investigations take longer. This is unlikely to change, given projected staffing and resource levels for personnel security operations.

The response time for many kinds of criminal fingerprint checks needs to be much faster. Police usually bring formal charges before a local magistrate within several hours after arrest. The results of an FBI fingerprint check of an arrestee frequently need to arrive within 2 to 4 hours to be useful. A prior criminal

[50] The FBI estimated a FY2000 daily volume of 62,300 cards, after verifying user survey results and assuming 50-percent NFF/III implementation by FY2000. The FBI initially estimated a daily volume of 74,000 cards with no NFF/III and 49,000 with full NFF/III. The unverified user survey results suggested a volume as high as 100,000 cards per day.

[51] The FBI subsequently adjusted its estimate from about 100,000 fingerprint cards per day, based on the unverified survey results, to 78,000 cards per day with no NFF/III, after verifying the survey results and correcting for double counting, purely speculative projections, and other anomalies.

record could be a significant factor in the magistrate's decision to release the arrestee on his/her own recognizance, set appropriate bail, or detain the arrestee in jail. A quick response is also needed to identify arrestees who may be wanted for criminal offenses in other States and jurisdictions. Fingerprint checks conducted for other criminal justice purposes, such as prosecution, sentencing, or parole decisions, usually do not require a rapid response. A response time of several days could be adequate. Under the NFF/III concept, at most only about 35 percent of arrestees would require an FBI fingerprint check in the first place. About 65 percent can be expected to have a prior local or State criminal record. Only first-time offenders in the arresting State would require a full FBI fingerprint check. All others would be positively identified at the local or State level and would already have State and Federal criminal identification numbers assigned (backed up by previously submitted fingerprints).

The implication is that the Ident automation program could more than meet criminal and noncriminal justice response time requirements with an overall average response time of about twice what is currently planned—this is still a dramatic improvement over current response times. The FBI's response time goal thus could be relaxed and still meet user needs. However, the FBI has determined that longer average response times would create queuing problems.[52] The FBI has set the 2-hour criminal and 24-hour noncriminal justice response time goals to balance the overall workload and handle peak demands without creating significant backlogs. OTA and independent experts concur that the system should be designed to avoid backlogs. The FBI has reserved weekend and night-shift operations for system maintenance. These times could be used to process any temporary backlogs that might occur, although the system is being designed to avoid backlogs altogether.

These response times are for Ident processing, and do not include mail delays—which can add several days or weeks. Live scanning and electronic transmission of fingerprints are the proposed long-term solutions to eliminate mail delays. Their technical feasibility has been proven, although necessary standards are still being developed. Many Federal agency users of Ident services[53] seem enthusiastic about acquiring live scan equipment and taking full advantage of electronic transmission, which, they believe, would dramatically improve overall response time by cutting out mail delays and by reducing or eliminating bureaucratic delays in the agencies.

Federal civilian agencies, for example, typically route fingerprint checks through their own personnel security offices, then to OPM's personnel investigations processing center (or to DIS, if checking military or defense contractors), and finally to the FBI. The results of the fingerprint checks have to follow these steps back to the original requesting agency. This explains why checks can take 45 to 60 days or longer to get to the end user, even though Ident may be processing them in 15 to 20 days.

Assumptions About File Size

The plan needs to make assumptions about the size of Ident fingerprint files needed to support four kinds of fingerprint matches:

1. 10-print against 10-print fingerprints (incoming fingerprints of persons arrested are compared with fingerprints of prior offenders already on file),
2. latent prints against 10-print fingerprints in a latent cognizant file[54] (latent prints from a crime scene are compared with fingerprints of prior offenders),
3. 10-print fingerprints against unsolved latent prints (incoming fingerprints of persons arrested are compared with unresolved latent prints), and
4. latent prints against unsolved latent prints (incoming latent prints are compared with unsolved latent prints already on file).

By far the largest file is the 10-print file, which stores fingerprints on known criminal offenders. Although it is known as the 10-print file, prints for all 10 fingers are not necessarily included. Some States store fingerprints on only 2 or 4 fingers, in order to reduce storage costs. Two- or 4-finger prints are usually sufficient for

[52]Ident plans to operate 7 days a week, but all volume estimates (including OTA's) are based on a 5-day work week. If the system is designed to a 5-day week, with some built-in margin of safety, the weekends would provide an extra margin for eliminating any temporary backlogs that might result from exceptionally high peak loads.

[53]Including INS, OPM, DIS, the Census Bureau, FAA, and the Secret Service.

[54]Technically, 10-print fingerprints suitable for matching against latent prints are known as "latent cognizant" fingerprints, which for large fingerprint volumes can be retained in a subset of the 10-print file known as a "latent cognizant file."

10-print against 10-print searches, but not for comparison with incoming latent prints. The FBI plans to store images for all 10 fingers, to support a latent cognizant file and for archival purposes.

The Ident criminal 10-print fingerprint file currently contains prints on about 24 million persons. The FBI initially assumed that file size will grow to about 34 million persons in 2000, presumably based on some growth in first-time arrestees plus the addition of some portion of the prints on repeat offenders not previously submitted at the time of initial arrest. The 34 million would allow a margin for additional baseline growth in the criminal population (up to the historical rate of 3 percent per year) plus submission of a limited number of missing prints,[55] but it is possible that a file of this size would not be adequate beyond 2000. The FBI now projects that a fiscal year 2000 10-print file size of 43 million is more realistic. This revised estimate is based on user survey results and higher estimates of the number of missing prints.

Some States have found that large numbers of fingerprint arrest cards were never reported to State repositories and thus are likely missing from the FBI file.[56] Not all offenses are reportable to State and FBI repositories, but crime statistics suggest the possibility of significant underreporting. The FBI estimates that 14.3 million total arrests were made in 1989.[57] Of these, roughly 6.1 million were reportable to the FBI (after deducting juvenile and nonserious misdemeanor offenses).[58] The FBI received about 4.4 million criminal fingerprint cards in 1989, which suggests a shortfall of about 1.7 million cards. With full NFF/III implementation, the shortfall would be about 0.6 million per year (35 percent of 1.7 million), or 3.6 million over the 1995 to 2000 time frame. This number assumes about three arrests per offender, on the average, and that arrest cards for repeat offenders would not be reportable. But NFF/III may be only half implemented by 2000, in which case the 43-million-person 10-print file size could be needed to accommodate the additional submissions.[59]

The FBI currently receives about three fingerprint cards per person, but only one fingerprint card per person is retained. All other cards are discarded or returned to the States after microfilming. This procedure would be unchanged with NFF/III, except that the primary images would be received and stored as electronic fingerprint images on optical disk rather than as paper fingerprint cards in filing cabinets.

The FBI must also determine the size of the latent cognizant fingerprint file, against which incoming latent prints can be compared. The 24-, 34-, or 43-million person file discussed above is known as the 10-print fingerprint file. This file is designed for storing 10-print fingerprints coming into the FBI for later comparison with other fingerprints. The matching of fingerprints is actually done by comparing fingerprint minutiae (e.g., details on the location of fingerprint characteristics). State and Federal AFIS experience indicates that matching 10-print fingerprints with each other works extremely well, with very high accuracy levels, when minutiae from only 2 or 4 fingers (usually the thumbs and forefingers) are compared.

The more difficult challenge is matching latent prints from crime scenes against the latent cognizant fingerprint file. Latent prints are single or partial fingerprints lifted from door handles, glasses, walls, firearms, clothing, and other items found at or near the scene of a crime. The latent print contains much less information than a standard 10-print fingerprint. To compensate, the number of fingers and the number of

---

[55]At 3-percent annual growth, a file of 24 million persons would grow to 32.25 million in FY2000. This would allow a margin of 1.75 million for the addition of missing fingerprints.

[56]Comprehensive data are not available. The FBI may wish to more systematically survey the States on unreported and unfiled criminal fingerprint cards.

[57]FBI, *Crime in the United States...1989*, op. cit., footnote 38, p. 172.

[58]14.3 million less 2.15 million juvenile arrests (estimated at 15 percent of the total) and 6.1 million nonserious misdemeanor arrests (defined for estimating purposes to include vandalism, liquor law violations, drunkenness, disorderly conduct, vagrancy, curfew and loitering violations, runaways, and all other) equals 6.1 million reportable arrests. These are gross approximations, since some juvenile offenses (when the offender is charged as an adult) and some nonserious misdemeanor offenses (e.g., for repeat offenders depending on State law) not included in the 6.1 million may be reportable. In addition, some serious misdemeanors (e.g., simple assault, stolen property, drug abuse violations) included in the 6.1 million may not be reportable (e.g., for first-time petty theft offenders, depending on State law). See FBI, *Crime in the United States...1989*, op. cit., footnote 38, pp. 172, 176.

[59]Eventually the growth rate of the 10-print file size should decline to that of the underlying growth in criminal activity, currently about 3 percent per year. If two out of three crimes are committed by repeat offenders, then the growth rate of new offenders added to the 10-print file (not old offenders previously unreported) would be about 1 percent per year if present trends continue.

minutiae on the fingerprints for the latent cognizant file must be increased to produce satisfactory search accuracy. This is typically done by extracting minutiae on all 10 fingers and creating a separate latent cognizant file that can be used for searching latent prints. Thumbs and forefingers alone would not suffice for comparison with latent prints, which could be from any finger.

The cost of storing and searching a latent cognizant file is much higher than the cost of storing and searching a 10-print file. The FBI found that extracting, storing, and searching for the additional fingerprint minutiae for all 24 million persons in the criminal 10-print fingerprint file (or the 34 to 43 million persons projected for 2000) would be prohibitive in cost. Current FBI plans propose a latent cognizant file on about 10 to 13 million persons (one-third the size of the 10-print file), selected to include serious multi-state offenders, with priority placed on violent offenders. Since Ident is planning to store full fingerprint images, the latent file could be expanded or modified in the future if technically and financially feasible. The ultimate size, composition, and geographic coverage of the FBI's latent cognizant file needs careful consideration to make sure that the file meshes with related State, regional, and local efforts and optimizes the Federal role. Decisions on the latent cognizant file are especially important in light of the high rate of success of automated latent searches conducted at the State/regional/local level. Many States report that old and/or difficult criminal cases have been solved due to latent matches that could not have been conducted manually (see boxes A and D).

Assumptions About Storage Requirements

The plan must make assumptions about the storage requirements for each set of fingerprints in the file. The FBI needs to store the entire image of each fingerprint to facilitate the extraction of minutiae by whatever vendor equipment the FBI ultimately procures and to permit fingerprint examiners to verify the minutiae-based candidate matches provided by the AFIS. With current technology, the AFIS identifies and ranks the most likely fingerprint matches, but a human examiner must make the final determination. Adequate image resolution can be provided at 500 pixels (picture elements) per inch, or 250,000 pixels per square inch, based on research conducted in support of the NIST image transmission standard-setting process. The standard fingerprint card includes 5 rolled finger blocks, 1 four-finger block, and 1 thumb block per hand, or a

Box D—Cal-ID: An Early Success Story

The automated latent cognizant fingerprint database of the California Identification (Cal-ID) system became operational on October 9, 1985. Automated latent fingerprint searches have proven effective in helping solve old or difficult cases. During the first year of operation, over 100 California law enforcement agencies used the latent database to identify criminal suspects:

- The Los Angeles Police Department used the Cal-ID latent system to identify and arrest four suspects in the kidnapping and execution-style murder of two college students, based on a latent print lifted from the victims' vehicle.
- The Sacramento County Sheriff's Department used Cal-ID to identify and arrest a suspect in the murder of a Sheriff's Department employee, based on a bloody latent print found at the crime scene.
- The San Diego County Sheriff's Department used Cal-ID to identify and arrest a suspect in a 3-year-old rape case, which led to the identification of the suspect as a serial rapist.
- The Anaheim Police Department used Cal-ID to identify and arrest a suspect in a 9-year-old homicide case.
- The Marysville Police Department used Cal-ID to identify and arrest a suspect in a 2-year-old homicide case.
- The Los Angeles Police Department used Cal-ID to identify and arrest a suspect in the axe attack and robbery of the California Secretary of State, which led to identification of the suspect in connection with numerous other robberies and burglaries.

SOURCE: California Department of Justice, *California Identification (CAL-ID) System and Remote Access Network (RAN) Status Report: 1986* (Sacramento, CA: California DOJ, Division of Law Enforcement, Bureau of Criminal Identification, 1987).

total of 14 blocks. Fingerprint images in these blocks typically cover about 24 square inches,[60] which equates to 6 million pixels per fingerprint.[61] The total block size (including white space) is about 39 square inches (or a maximum of 9.8 million pixels).[62]

The FBI could store on optical disk the images of fingerprints using various gray scales, ranging from binary (black and white only) to 16, 64, or 256 shades of gray. The emerging industry norm seems to be to store images of all 10 fingers on a 256 gray scale. Eight bits or 1 byte per pixel are required to capture a 256 gray scale. Minutiae may, in comparison, be extracted and stored for as few as 2 or 4 fingers for the 10-print file, and 8 or 10 fingers for the latent cognizant file.

The FBI plans to store the images of all 10 fingers in order to have a complete electronic fingerprint archive. This would provide full backup and permit the possible expansion of the latent cognizant file at a future time, should technology and resources permit. The FBI, NIST, and vendors are working on data compression techniques to reduce the image storage requirements. A compression ratio of 8:1 provides acceptable image quality with existing technology; the FBI expects that compression ratios of 15:1 or greater will be feasible with new methods. Thus the image data per fingerprint card will be reduced from 9.8 megabytes to at most 1.2 megabytes (at 8:1 compression), and probably to 0.65 megabyte (at 15:1 compression) or less.

---

[60](1.25 square inches x 10 rolled finger blocks) + (0.94 square inches x 2 four-finger blocks) + (4.5 square inches x 2 thumb blocks) = 12.5 + 1.88 + 9.0 square inches = 23.38 square inches per fingerprint card.

[61]250,000 pixels per square inch x 24 square inches = 6 million pixels per fingerprint card.

[62]FBI estimate.

The FBI plan should consider the implications of various design factors for technical risk, schedule, and cost. Qualitatively, design parameters such as fingerprint volume, response times, fingerprint file sizes, and fingerprint storage requirements will affect the technical and schedule risk and automation cost.

The plan should weigh the risks and costs of delays that might result if system requirements exceed available technical capabilities. The FBI's desire to regain technological leadership in the fingerprint identification field is commendable. The current system is technically obsolete and incompatible with State systems. Even implementation of today's state of the art, or the state of the art as it might exist when requests for proposals are solicited and contracts awarded, should be a significant improvement over the status quo. The plan should provide for an easy upgrade to the system as technology advances and as needed if fingerprint storage and processing volumes exceed design capacity. A modular upgrade strategy may be especially appropriate in light of uncertainties about possible major new noncriminal justice needs for fingerprint checks.

The FBI planning process needs to consider several alternatives simultaneously to help the user community and Congress, as well as the FBI itself, to better understand the tradeoffs among different alternatives. In particular, the FBI needs to clearly show the tradeoffs among volume and type of fingerprint checks, technical design, cost, schedule, technical risk, number and type of employees, training needs, and building requirements. A full tradeoff analysis is needed prior to finishing the strategic plan and issuing the Request for Information—the next major steps toward procurement.

The FBI is conducting a tradeoff analysis with the assistance of Mitre Corp., but because of procurement sensitivity it does not, at this time, plan to make the results public. The type of analysis needed is illustrated below. This is, of course, no substitute for a complete FBI study released in a format that both protects the integrity of the procurement process and better informs the public and Congress.

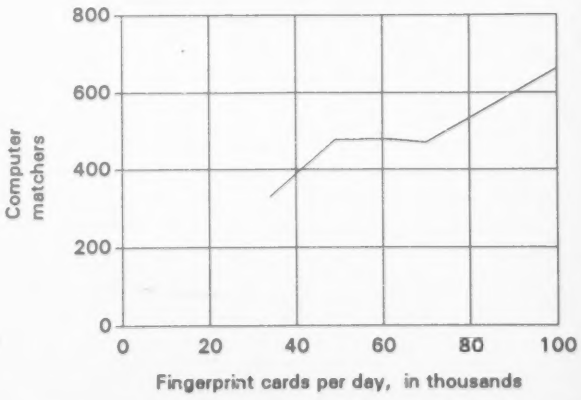
Illustrative Review of Ident Automation Costs

Computer Matcher Requirements

The analysis could begin by focusing on the number of computer matchers needed to handle the projected Ident 10-print workload. Matchers are computers that compare the minutiae of incoming fingerprints against the minutiae of prints on file. The projected workload is primarily a function of assumptions about processing volume (fingerprint cards or electronic images received per day), response (or turnaround) time, and file size. Projections of fingerprint processing volume range from 100,000 to 34,000 (see table 7). For this illustration, response time is assumed to be 2 hours criminal and 24 hours civil, and file size is assumed to be 34 million.

Roughly 480 matchers would be needed to process 61,000 fingerprint checks per day (the OTA-4 scenario) against a 34-million-fingerprint file—using 1990 technology.[63] A higher or lower daily volume would, other things being equal, increase or decrease the number of matchers required. Technical advances could, in the

Figure 8—Projected Number of Ident Computer Matchers, 2000



NOTE: See table 8 and accompanying text for detailed explanation. Assumes 1990 technology; technical advances are likely to reduce the number of matchers required to process any given volume of fingerprint cards

SOURCE: Office of Technology Assessment, 1991.

[63]OTA estimated the number of matchers for this illustration based on vendor assumptions about scaling up from the California AFIS. California uses about 5 matchers to process 5,000 10-print searches per day comparing 2 fingers per print against a file of about 8.5 million prints.The illustrative Ident system would process 61,000 searches per day (about 12 times the number processed by California), comparing 4 fingers (2 times the number compared by California) against a file of 34 million prints (about 4 times the size of the California file). Thus the estimated baseline number of Ident matchers is 5 x 12 x 2 x 4 = 480.

Table 8—Number of Computer Matchers Required by Year 2000, as a Function of Daily Fingerprint Submissions

Daily card submissions, FY 2000[a]	Criminal matches[b]	Civil matches[b]	Total matches[b]	Number of matchers[b]
100,000 (OTA-6)	17,500	47,000	64,500	663
70,000 (OTA-5)	11,900	33,840	45,740	470
61,000 (OTA-4)	12,500	34,200	46,700	480
49,000 (OTA-3)	11,830	34,560	46,390	477
43,000 (OTA-2)	11,830	28,800	40,630	418
34,000 (OTA-1)	10,010	22,080	32,090	330

[a] From table 7.
[b] Number of matchers = (480)(matches at volume x ÷ matches at 61,000).

NOTES: All OTA scenarios assume the criminal/civil split shown in table 7.
OTA-1, OTA-2, and OTA-3 assume full NFF/III, 9-percent criminal name hit, and 4-percent civil name hit.
OTA-4 assumes half NFF/III, 50-percent criminal name hit, and 5-percent civil name hit.
OTA-5 and OTA-6 assume no NFF/III, 65-percent criminal name hit, and 6-percent civil name hit.

SOURCE: Office of Technology Assessment, 1991.

future, reduce the number of matchers needed for any given volume of matches and fingerprint checks.

The OTA-1 estimate of daily fingerprint card submissions (34,000) would reduce the number of matchers by about one-third (to 330), other things being equal (see table 8 and figure 8). The OTA-2 estimate (43,000 cards per day) would reduce the number of matchers by about 12 percent (to 418). The OTA-3 and OTA-5 scenarios (49,000 cards per day with full NFF/III, and 70,000 with no NFF/III, respectively) would reduce the number of matchers only slightly. The OTA-6 scenario (100,000 cards per day) would increase the number of matchers by more than one-third (to 663 matchers). An important caveat: This illustrative analysis assumes linear relationships among volume, number of matches, and number of computer matchers. Any nonlinear relationships, or any economies or diseconomies of scale, could change the results.

The results suggest that Ident could significantly reduce the number of matchers only by designing for a lower daily volume of noncriminal justice fingerprint checks (see table 8). The number of criminal checks does not have much effect on the number of matchers (except under the very high OTA-6 estimate), since the number of actual criminal matches is essentially the same whether the NFF/III is implemented or not. The NFF/III simply shifts the much less costly name hits from Ident to the States. The impact of technical advances, however, could be much greater. Vendors estimate that the number of matchers might be reduced by 25 percent with 1991 technology and by 50 to 90 percent with 1993 technology (the year planned for actual procurement), other things being equal.

An analysis of the number of matchers required to handle projected latent matches shows similar results. The FBI has assumed a daily volume of 128 latent fingerprint searches in 2000. The number of latent print matchers could be reduced if the volume of latent searches is smaller. Many States have or are obtaining their own automated latent search capabilities. These States run latent prints against their own latent cognizant files first, thus substantially reducing the primary demand for FBI latent searches. Nonetheless, the payoff from successful latent searches is very high, and AFIS is the only viable means of conducting large-scale latent searches. The number of latent searches conducted by Ident has actually declined from about 90 per day in fiscal year 1981 to 50 per day in fiscal year 1990. The FBI believes that this trend reflects the severe limitations of Ident's current latent processing system, and that demand would rebound once Ident offered a state-of-the-art service. The 128 latent searches per day projected for fiscal year 2000 seems reasonable, if the real base is the 90 per day of fiscal year 1981. A reduction in matchers is more likely to result from technical advances.

This illustrative analysis focuses first on the computer matchers because they are the most expensive and technically complex components of AFIS systems. The matchers also are the most affected by volume.

The number and size of optical disk storage devices, for example, are determined largely by the size of the Ident fingerprint file (and the number of fingerprint images that need to be stored) and by the gray scale and data compression ratios (which determine the number of bytes of data per image stored). The number and size of magnetic tape or disk drives likewise are a function of the fingerprint file size (and the number of minutiae extracted per finger and fingerprint). The FBI's tradeoff analysis should cover all major AFIS components, including optical, tape, and disk drive storage as well as the matchers.

Building Construction Requirements

The FBI should analyze the implications of technical tradeoffs for building requirements. The FBI is planning for a 46,500-square-foot Ident computer center at the new Clarksburg, West Virginia, location.[64] The computer matchers, for example, typically account for over one-third of the total computer center space requirements—probably about 40 percent if peripheral equipment (e.g., controllers) and cooling units are included. The matchers typically account for perhaps half of the computer center's electric power needs.

Thus a hypothetical 20-percent reduction in the number of computer matchers, for example, could translate directly into an 8-percent reduction in computer center floor space and a 10-percent reduction in power requirements. A 50-percent reduction in the number of matchers, which may be possible with new technology, could cut floor space by about 20 percent and power by 25 percent. A 50-percent increase in matchers, needed for the OTA-6 scenario using 1990 technology, could increase floor space and power requirements by 20 and 25 percent, respectively.

The tradeoff analysis also should show impacts of volume on other building requirements—primarily the new office complex that will house most of the Ident employees. The FBI has assumed, as a baseline, that the daily fingerprint volume will nearly double by 2000 and the workforce will remain about constant. The current workforce is 2,500 (down from over 3,000 a decade ago), with 479 additional positions requested starting in fiscal year 1992 (to reduce the fingerprint and disposition backlog, and to convert remaining manual criminal history records). The new office complex has been designed to accommodate 3,000 persons plus common areas (e.g., a cafeteria and auditorium).[65]

If the year 2000 daily volume is significantly less than projected, some reduction in staffing would be expected. This reduction would in turn reduce the required size of the new office complex. However, a lower projected daily volume does not translate directly into lower staffing requirements, since some staff functions do not vary much as a function of volume. Assume, for illustrative purposes, that one-third of the staff are fixed and the other two-thirds variable, that the variable staff changes in proportion to the absolute volume of fingerprint checks requested, and that 3,000 persons are required to process 61,000 fingerprint cards per day (with half implementation of NFF/III, as in the OTA-4 scenario).

Staffing levels would range from a low of 2,100 persons at 34,000 cards per day to a high of 4,300 persons at 100,000 cards per day (see table 9 and figure 9). A daily volume of 49,000 fingerprint cards, rather than 61,000, in the year 2000 would require a staffing level of about 2,600 persons, rather than 3,000. This could reduce the office requirements from 488,000 square feet to about 425,000 square feet—a reduction of about 13 percent (see table 9). A daily volume of 100,000 cards, rather than 61,000, would, in contrast, increase staffing and floor space by about 43 percent. The FBI's tradeoff analysis should more completely specify the staffing levels and required office-complex floor space for a range of fingerprint volume scenarios.

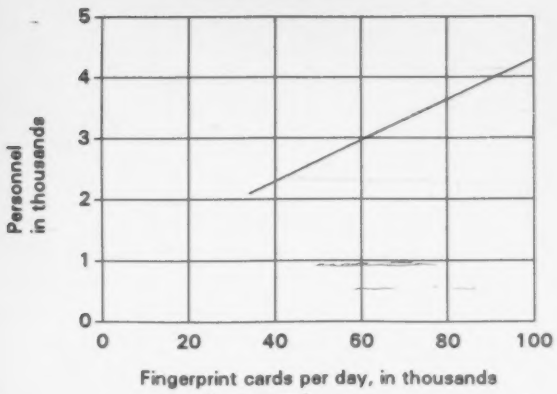
Impact on Ident Costs

Reductions in the number of computer matchers combined with reductions in computer center and office space needs could significantly reduce Ident costs. Increases in the number of matchers and office space needs, on the other hand, could increase costs. Cost reductions or increases could be approximated as follows. First, assume that Ident modernization costs $200 million for building construction (including design, inspection, taxes, and contingencies) to accommodate a volume of 61,000 cards per day. Second, assume that the office complex typically costs about 42 percent of the construction total, and the computer center about 18 percent. Third, assume that the computer

[64]The total computer center size is actually 93,000 square feet, divided between two floors; only one floor is currently planned for Ident AFIS.

[65]With 488,000 gross square feet, the facility would be slightly larger than current Ident space in the Hoover Building (330,000 ft^2) and two other buildings (110,000 ft^2).

Figure 9—Projected Number of Ident Personnel, 2000



NOTE: See table 9 and accompanying text for detailed explanation.

SOURCE: Office of Technology Assessment, 1991.

Table 9—Scenarios for Ident Fingerprint Volume, Staffing, and Office Complex Requirements, Year 2000

Daily card submissions	Approximate staffing levels[a]	Office complex floor space (gross sq. feet)
100,000 (OTA-6)	4,300	620,000
70,000 (OTA-5)	3,300	540,000
61,000 (OTA-4)	3,000	488,000
49,000 (OTA-3)	2,600	425,000
43,000 (OTA-2)	2,400	390,000
34,000 (OTA-1)	2,100	340,000

[a] Assumes personnel are one-third fixed, two-thirds variable, and that a daily volume of 61,000 cards requires a staff of 3,000 persons.

SOURCE: Office of Technology Assessment, 1991.

matchers cost about $100 million (for 1990 technology).[66] The cost savings (increase) at lower (higher) projected daily volumes can then be estimated in proportion to lower (higher) estimates of the requirements for computer matchers, staffing levels, and computer center and office complex space.

This illustrative analysis of the sensitivity of cost to various assumptions about volume suggests that the matcher cost component is quite sensitive. Lower volume (OTA-1 or OTA-2 scenario) reduces the number of matchers needed, with savings in the $2 million to $30 million range (see table 10). Higher volume (OTA-6 scenario) could increase matcher cost by $40 million. The office complex cost is a function of volume and staffing: lower volumes and staffing levels (OTA-1, OTA-2, OTA-3) reduce the space requirements, with possible savings in the $11 million to $25 million range. High volumes and staffing levels (OTA-5, OTA-6) could increase the office cost by up to $23 million. The computer center cost varies with daily volume and the number of matchers required. Lower volume and fewer matchers mean smaller space requirements, with a possible savings of up to $4 million. Higher volume and more matchers could increase costs by $5 million.

The analysis illustrates that costs for the computer matchers and computer center are not very sensitive to changes in daily volume within the range of 49,000 cards with full NFF/III implementation to 70,000 cards with no NFF/III implementation. This is because the actual number of full fingerprint searches and matches required (as compared with name checks of prior offenders and simple fingerprint verifications) is about the same at 49,000 cards with full NFF/III implementation, 61,000 cards with half NFF/III implementation, and 70,000 cards with no NFF/III implementation. A name check hit is confirmed by comparing the person's new fingerprint card (or image) for the current arrest with the card (or image) on file from prior arrest listed for that person, rather than having to conduct a search of the entire fingerprint file. With no NFF/III, these name checks and fingerprint verifications would be conducted by Ident. With full NFF/III, the States would do the name checks and verifications.

In this range, significant cost savings are more likely to result from technical advances in computer matchers (and related equipment) and, to a lesser extent, from smaller office complex requirements at the lower volumes and staffing levels.

Total potential savings for these three cost components range from about $30 million to $60 million (for the OTA-2 and OTA-1 scenarios, respectively), against a base of $220 million—a possible savings in the 14- to 28-percent range (figure 10). The potential increases for these cost components could be as much as $67 million, or 30 percent, for the OTA-6 scenario. The

[66] Assumes a cost of about $210,000 per matcher with a volume discount. Some 1991 matchers cost in the range of $350,000 each but have twice the processing capacity, for an effective cost of $175,000 for equivalent matcher capacity.

Table 10—Scenarios for Ident Daily Fingerprint Volume, Response Time, Matchers, and Cost

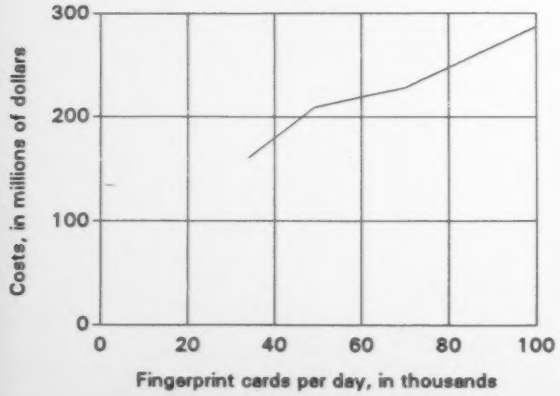
Daily volume	Number of computer matchers	Matcher cost	Computer center cost[a]	Office complex cost[b]	Total cost[c]
100,000 (OTA-6)	663	$139M	$41M	$107M	$287M
70,000 (OTA-5)	470	$ 99M	$36M	$ 93M	$228M
61,000 (OTA-4)	480	$100M	$36M	$ 84M	$220M
49,000 (OTA-3)	477	$100M	$36M	$ 73M	$209M
43,000 (OTA-2)	418	$ 88M	$34M	$ 67M	$189M
34,000 (OTA-1)	330	$ 70M	$32M	$ 59M	$161M

[a] Includes prorated share of other costs. Assumes matchers (including controllers and cooling units to support them) account for 40 percent of computer center space. Assumes $22M is fixed cost.
[b] Includes prorated share of other costs. Total cost is proportional to floor space (See table 9).
[c] Includes matcher, computer center, and office complex costs.

SOURCE: Office of Technology Assessment, 1991.

cost differences between OTA-3, OTA-4, and OTA-5 are less significant. Matcher and computer center costs do not appear to be very sensitive to daily fingerprint volume within the 49,000 to 70,000 range, due to the effects of NFF/III. Other automation components, including image processing and minutiae extraction systems, minutiae editing work stations, data entry terminals, scanners and printers, and telecommunications input/output equipment and line capacity, may be more sensitive.

Figure 10—Projected Illustrative Ident Automation Costs, Selected Items



NOTES: Costs shown are for computer matchers, computer center complex, and office complex only. See table 10 and accompanying text for detailed explanation.

SOURCE: Office of Technology Assessment, 1991.

The FBI tradeoff analysis should estimate potential savings (or cost increases) in the total automation budget, which can be roughly estimated as follows. Assume first that the total automation cost breaks down into 50 percent for AFIS (25 percent for matchers, 25 percent for other AFIS equipment); 25 percent for criminal record computers (including III computers); and 25 percent for telecommunications.[67] Assume second that the matcher cost is $100 million (for 1990 technology). This suggests a total baseline automation cost of $400 million to accommodate the OTA-4 scenario (61,000 cards per day). Technical advances should reduce the cost of the system somewhat if bought today, and more substantially by the time the contract is actually awarded (planned for fiscal year 1993). To develop an authoritative analysis, the FBI needs to carefully examine the cost impact of assumptions about overall volume, NFF/III participation, and the ability of users to transmit fingerprints electronically. The results should provide a better understanding of how the FBI might reduce, to the extent possible, costs of the AFIS, computer, and telecommunication capabilities needed to support Ident modernization. The results also should help the Administration and Congress better understand what capabilities can be purchased at various levels of funding.

The tradeoff analysis also should consider implications for the composition as well as the size of the workforce, for employee training, and for technical and schedule risk.

[67] Typical split for integrated AFIS/CCH systems at the State level, based on vendor estimates.

Composition and Training of Ident Workforce

Over time, Ident will have fewer employees doing manual tasks, and more employees working directly with computer terminals and systems. The skill requirements will increase further for those already working with computers. Thus Ident will need an active retraining program for current employees and training for new employees. The balance between retraining and new hires will depend on total staffing requirements, number of current employees electing to move to West Virginia, employee attrition (retirements, separations, transfers to other FBI divisions), rate of transition from manual to electronic processing; and rate of implementation of NFF/III.

OTA's analysis of Ident job titles and staffing complements (as of Mar. 25, 1991) indicates significant retraining needs, for example:

- Identification record clerks doing typing will need to be retrained for computer terminal operation.
- Mail and correspondence clerks will need to be retrained for electronic mail and electronic filing/processing operations.
- Most arrest record examiners and assistants will no longer be needed with full NFF/III and will have to be phased out through attrition or retrained for other jobs.
- Coding clerks will need to be retrained for new AFIS/III systems.
- Fingerprint examiners will need to be retrained for new AFIS systems. The number needed will be a function of processing volume.

The majority of current Ident employees who elect to move to West Virginia will need retraining. New hires will need more intensive and computer-oriented training than in the past. Supervisory personnel at all levels will need not only retraining in the relevant technical skills but also training in changing to a high-tech organizational setting. This will be especially challenging for the supervisory coding clerks (64) and supervisory fingerprint examiners (110) who will have to contend simultaneously with changes in their own jobs and those of their employees. In addition, employees moving to West Virginia will have to manage their own personal relocation as well.

Ident will need a new cadre of in-house trainers, possibly supplemented with outside assistance for the

Box E—Ident Automation: A Necessary Risk

The Ident automation program is high risk because of the combination of technical, personnel, and building requirements:

- The new automated fingerprint identification system (AFIS) must process a much larger daily volume of fingerprint checks against a much bigger fingerprint file than even the largest State AFIS.
- The Ident automation schedule calls for designing, procuring, and implementing the new AFIS in the time frame typically needed for smaller State systems.
- The Ident building schedule calls for construction (in Clarksburg, West Virginia) to proceed faster than normal for a facility of this size and complexity.
- The Ident personnel schedule calls for moving perhaps 750 to 1,000 employees (to West Virginia), hiring 1,500 to 2,000 new employees, and training all employees in a compressed time frame.

But the Ident automation program is a necessary risk because:

- the current Ident fingerprint identification system is technically obsolete (and should be completely phased out);
- the current Ident system is too slow to meet many criminal justice and nonjustice needs for fingerprint checks;
- the current Ident building space (at the J. Edgar Hoover Building in Washington, DC) is inadequate for making the transition to a fully automated system; and
- the current Ident workforce has experienced high turnover and low morale due in part to less competitive salaries and long commutes (in the high cost Washington, DC, area).

Ident therefore needs to give special attention to managing the risks of the entire revitalization process (automation, construction, moving, training), and should be prepared to make adjustments as new information becomes available.

Ident has an opportunity to break with the past and establish a new, state-of-the-art facility with a reenergized workforce. A modernized and revitalized Ident will help meet the Nation's criminal identification and records infrastructure needs at and beyond the turn of the century.

SOURCE: Office of Technology Assessment, 1991.

transition. Ident's current complement of nine fingerprint examiner instructors and two identification record instructors could be upgraded and expanded. These instructors would themselves need retraining. Additional trainers might be drawn from the ranks of the most senior, most experienced fingerprint specialists (75) and supervisory fingerprint specialists (22). Another possibility would be to involve the current group of computer personnel, including 24 computer operators, 20 computer programmers (all types), 26 computer system analysts, 5 computer scientists/specialists, 3 electronics engineers, and 15 electronics technicians. Again, retraining the trainers would be a necessity.

Technical and Schedule Risk

The tradeoff analysis also needs to consider the implications for technical and schedule risk (see box E). The Ident modernization plan is, as it stands, on a rigorous schedule. The building construction time table requires that decisions on the size of the computer center be made within the next few months. Bid packages for the computer center and central plant are to be issued in late 1991 or early 1992, with construction to begin in spring 1992. Bid packages for the main office building will be issued in spring 1992, with construction to begin in the summer and to be completed in late 1994. Some parts of the computer center and office complex are to be ready by April 1994, so phased occupancy can take place between spring 1994 and spring 1995. Full operation is planned for June 1995.

The building construction schedule is tight, but it allows some margin for slippage and depends on straightforward, proven construction techniques. The technical risk for the building is small, and most, if not all, of the necessary funding has already been appropriated by Congress.

The automation schedule, in comparison, is very tight and allows little if any margin for error. Further, the technical risk is inherently high, given the unprecedented scope and scale of the project. (By way of comparison, this project involves a file size about 3 to 5 times that of the California AFIS, a daily volume 7 to 12 times higher, and many additional features.) Little of the necessary funding for automation has been approved by Congress.

The current automation schedule is as follows: automation strategy decision, summer-fall 1991; Request for Information (RFI) issued to all interested vendors, fall 1991; Request for Proposal (RFP) issued to selected best qualified vendors, early 1992; prototype demonstrations by the most qualified vendors, mid to late 1992; contract award, early 1993; begin system installation, spring 1994; full operation, June 1995. The schedule allows little room for delays for any reason. The schedule is essentially a series of critical paths; delays at any point would be carried along to each subsequent step in the process. The time between contract award and full operation (about 27 months) is in the same range required for procurement and installation of systems at the State level (typically 18 to 30 months). Ident is proposing to do a much larger, more complicated system procurement and file conversion in about the same time, and with the further complicating factors of moving to a new building hundreds of miles away (although the move offers other advantages), relocating existing employees, hiring new employees, and training virtually all employees.

The move should, however, help the FBI develop a more stable, higher quality Ident workforce. Ident has in the past experienced high turnover and low morale at its current Washington, DC, location, in part because the high cost of living and comparatively low salaries require many Ident employees to commute long distances. Ident has difficulty filling vacancies with qualified persons. Ident expects salaries to be more competitive, living costs lower, and commutes shorter in West Virginia. As of September 3, 1991, over 7,000 new applicants had applied for the first 200 positions available at a satellite office opening in Clarksburg, West Virginia. Ident estimates that about one-third of the current workforce will elect to move to West Virginia and thereby provide a core staff for training and transitional purposes. (All current Ident employees who choose not to move have been guaranteed continued FBI employment in the Washington, DC, area at no loss of pay.)

The risks of moving to an area with a lower cost of living and a potentially more stable, motivated workforce seem necessary, given the current staffing problems. In addition, Ident's present home (the J. Edgar Hoover Building) is overcrowded and considered unsuitable for a fully automated Ident, especially since the transition will probably require several years of dual operation of the old and new systems. It

appears much easier to phase the new system in at a new location, and the old system out at the current location, rather than try to do both at the same location.

Moving an agency can be an important part of organizational change and renewal, as seems to be the case for Ident. The move to West Virginia should help Ident break with the past and establish a new, state-of-the-art facility with a reenergized workforce. The existing facility in Washington, DC, and its obsolete system will not be moved to the new location, but instead will be phased out over a transitional period. Current Ident employees who choose to move will, inevitably, face some stress in adjusting to a small-town or rural environment. Ident has hired human resource consultants to assist with the transition.

The move also illustrates the decentralizing potential of electronic technology. With a manual fingerprint process, Ident had to be located in close physical proximity to other FBI laboratory and investigative operations. In the electronic era, Ident can be located at a remote site, since fingerprints can be transmitted electronically and instantaneously between Clarksburg, West Virginia, Washington, DC, and law enforcement agencies around the country.

Some technical risk also is justifiable, since it is unclear whether simple extension of current technology can meet Ident needs. Vendors claim they can meet these needs without resorting to entirely new technical approaches, but some users are skeptical. Pushing for new technology solutions can be constructive, up to a point, but unproven systems are risky and potentially expensive. The FBI could reduce the technical risk after reviewing the RFI responses by using the RFP to procure the best commercially available technologies existing at the time of the procurement, rather than attempting to require significant additional R&D work by vendors as part of the procurement. Most vendors will do some development anyway, and will strive to provide the most advanced proven technologies possible. But if FBI requirements are such that substantially new and unproven technologies are required, then Ident would be faced with the prospect of significant shake-down and break-in problems associated with all new systems (including hardware and software debugging). On the down side, Ident could face serious delays and budget overruns, with no guarantee that additional funds would be available.

If new technology solutions are not clearly evident after the RFI, the lower technical risk strategy then would be for Ident to: 1) push for the next generation of current systems, which would be more powerful and cost-effective, but which will be technically proven and commercially available in the 1993 to 1994 time frame; and 2) place the purely R&D work on a separate, longer term track pointing toward 2000 and beyond. The experience of Federal agencies that have attempted automation programs of this magnitude is that some problems will occur even with the best laid plans and proven technologies. But if the plan involves significant R&D and new technologies, the project is likely to encounter serious technical problems and schedule and cost overruns. This is true even for agencies with major continuing R&D programs. Ident does not have an extensive R&D track record. Making a long-term commitment to AFIS R&D may be desirable, but the real pay-off from R&D is typically 8 to 10 years or more in the future, not 2 to 3 years. Technical and schedule risk also could be lowered by reducing the demands on the automated system as much as possible.

Another option is to simply stretch the project out by 2 to 4 years. This would allow time for more R&D before procurement commenced. This option could, however, impact the cost of the project significantly. The cost of procuring the new system could increase due to inflation, perhaps in the range of $1 million per month—$667,000 for automation delays[68] and $350,000 for building construction delays.[69] Thus a 2-year delay could add as much as $48 million to the project cost. The cost of delay could be even higher, if, for example, the new system is less expensive to operate than the current system, and potential savings are foregone. A delay could, on the other hand, reduce costs if further technical breakthroughs resulted in a more cost-effective system with even lower net procurement and operating costs. The FBI does not believe that additional technical advances of this magnitude are likely even with a 2-year stretchout.

[68]$400 million times 6-percent escalation over the life of the project, divided by 36 months (FY92, FY93, FY94).

[69]$210 million times 6-percent escalation divided by 36 months (FY92, FY93, FY94).

Lack of funding could, of course, force a delay in the project. The new building construction is funded (against the current schedule), but the automation component is only partially funded (including some proceeds from Ident user fees). The Office of Management and Budget recommended zero funding for fiscal year 1992.[70] The FBI estimated that this would delay the automation program by 16 to 18 months, at an additional cost of $11 to $12 million. Congress is in the process of determining the fiscal year 1992 appropriation.[71]

The true cost of Ident automation delays—for whatever reasons—could be much larger, because delays prolong the unquantifiable but large number of criminal justice decisions made erroneously each day due to untimely or incomplete Ident fingerprint and criminal record checks. Ident fingerprint checks today cannot be completed fast enough for use in arrest, initial charging, or bail decisions. Even for sentencing decisions that have a longer lead time, Ident fingerprint and record checks could be incomplete because of the large backlog of unfiled arrest fingerprint cards and dispositions, and the 8.8 million Ident criminal history records not yet computerized (and not accessible via III). The FBI has requested fiscal year 1992 funds to begin clearing the backlogs and converting manual records. But these remedial actions will take years (about 2 years for backlog clearance, 4 years for records conversion), and offer only temporary improvement. The roughly 3 million unfiled dispositions represent only a small fraction of missing dispositions, which could total up to 36 million.[72] In addition, Ident is receiving a large number of duplicate criminal fingerprint cards, all requiring some amount of processing. In fiscal year 1990, Ident received and processed about 3 million criminal fingerprint cards that duplicated cards already on file. Ident fingerprint identification and record check deficiencies also are affecting nonjustice decisions.

The intangible costs of compromised criminal justice decisions and employment, licensing, and security clearance record checks seem far greater than any strictly monetary costs or benefits of delay. Nobody has quantified how many repeat serious offenders are inadvertently released because of misidentification or missing criminal history records, how many nonserious offenders are detained because of misidentification or incomplete records, or how many serious crimes are not solved because of the inability to conduct latent fingerprint searches. But the public safety and civil liberties costs of delay are, undoubtedly, much larger.

The long-term solution to duplicate, incomplete, or inaccessible fingerprint cards and criminal history records is full implementation of NFF/III, combined with further improvements in the automation and quality of State criminal records and a realistic, appropriately sized Ident automation program. The result should be a criminal records infrastructure that can meet the Nation's needs at and beyond the turn of the century.

---

[70]The Office of Management and Budget believed that the Ident system design and procurement process was not sufficiently far along to justify or require substantial FY92 expenditures.

[71]The Senate included an additional $48.0 million for Ident automation and $12.5 million for Ident record conversion and backlog reduction in the FY92 appropriations bill. The House included no additional funds. A Senate-House conference committee met to reconcile these and other differences. The conference committee agreed to the Senate funding levels, but with an additional requirement that the FBI set up an independent Ident automation and relocation program office that is completely separate from the Ident division itself. The committee provided $1.5 million for this purpose. See U.S. Congress, House, *Congressional Record*, Oct. 1, 1991, pp. H7171-7172.

[72]Ident receives dispositions on about half the arrests, so up to 36 million dispositions could be missing from the estimated 75 million criminal arrest events reportedly on file.

Superintendent of Documents **Publications** Order Form

Order Processing Code:
*** 6111**

Charge your order. It's easy!

To fax your orders and inquiries–(202) 275-0019

☐ **YES,** please send me the following indicated publications:

_____ copies of ***The FBI Fingerprint Identification Automation Program: Issues and Options (50 pages),*** S/N 052-003-01266-9 at $2.50 each.

☐ Please send me your **Free Catalog** of hundreds of bestselling Government books.

The total cost of my order is $_____. (International customers please add 25%.) Prices include regular domestic postage and handling and are good through 5/92 After this date, please call Order and Information Desk at 202-783-3238 to verify prices.

_____
(Company or personal name) (Please type or print)

_____
(Additional address/attention line)

_____
(Street address)

_____
(City, State, ZIP Code)

(_____)
(Daytime phone including area code)

Please Choose Method of Payment:

☐ Check payable to the Superintendent of Documents

☐ GPO Deposit Account ☐☐☐☐☐☐☐☐-☐

☐ VISA or MasterCard Account

☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

_____
(Credit card expiration date)

Thank you for your order!

_____
(Signature)

10/91

Mail To: Superintendent of Documents, Government Printing Office, Washington, DC 20402-9325

Office of Technology Assessment

The Office of Technology Assessment (OTA) was created in 1972 as an analytical arm of Congress. OTA's basic function is to help legislative policymakers anticipate and plan for the consequences of technological changes and to examine the many ways, expected and unexpected, in which technology affects people's lives. The assessment of technology calls for exploration of the physical, biological, economic, social, and political impacts that can result from applications of scientific knowledge. OTA provides Congress with independent and timely information about the potential effects—both beneficial and harmful—of technological applications.

Requests for studies are made by chairmen of standing committees of the House of Representatives or Senate; by the Technology Assessment Board, the governing body of OTA; or by the Director of OTA in consultation with the Board.

The Technology Assessment Board is composed of six members of the House, six members of the Senate, and the OTA Director, who is a nonvoting member.

OTA has studies under way in nine program areas: energy and materials; industry, technology, and employment; international security and commerce; biological applications; food and renewable resources; health; telecommunication and computing technologies; oceans and environment; and science, education, and transportation.

CONGRESS OF THE UNITED STATES
OFFICE OF TECHNOLOGY ASSESSMENT
WASHINGTON, D.C. 20510-8025

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
OFFICE OF TECHNOLOGY ASSESSMENT
379

OTA-BP-TCT-84

NOVEMBER 1991